SOLICITATION, OFFER AND AWARD

1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	RATING	PAGE	OF	PAGES
	DO-A7	1		104

2. CONTRACT NO.	3. SOLICITATION NO.	4. TYPE OF SOLICITATION	5. DATE ISSUED	6. REQUISITION/PURCHASE NO.
N6523619D1002	N65236-16-R-0001	[ ] SEALED BID (IFB) [X] NEGOTIATED (RFP)	13 Apr 2017	

7. ISSUED BY	CODE	8. ADDRESS OFFER TO (If other than Item 7)	CODE
US NAVY SPAWARSYSCEN ATLANTIC CHARLESTON PO BOX 190022 2.0 CONTRACTS 843-218-5941 CALVIN.HOWARD@NAVY.MIL NORTH CHARLESTON SC 29419-9022 TEL: 843-218-5941 FAX: 843-218-5947	N65236	**See Item 7** TEL: FAX:	

NOTE: In sealed bid solicitations "offer" and "offeror" mean "bid" and "bidder".

SOLICITATION

9. Sealed offers in original and 1 copies for furnishing the supplies or services in the Schedule will be received at the place specified in Item 8, or if handcarried, in the depository located in see L-349 until 02:00 PM (Hour) local time 22 May 2017 (Date)

CAUTION - LATE Submissions, Modifications, and Withdrawals: See Section L, Provision No. 52.214-7 or 52.215-1. All offers are subject to all terms and conditions contained in this solicitation.

10. FOR INFORMATION CALL:	A. NAME	B. TELEPHONE (Include area code) (NO COLLECT CALLS)	C. E-MAIL ADDRESS
	CALVIN HOWARD	843-218-5941	calvin.howard@navy.mil

11. TABLE OF CONTENTS

(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				**PART II - CONTRACT CLAUSES**	
X	A	SOLICITATION/ CONTRACT FORM	1 - 2	X	I	CONTRACT CLAUSES	82 - 103
X	B	SUPPLIES OR SERVICES AND PRICES/ COSTS	3 - 10			**PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACHMENTS**	
X	C	DESCRIPTION/ SPECS/ WORK STATEMENT	11 - 72	X	J	LIST OF ATTACHMENTS	104
	D	PACKAGING AND MARKING				**PART IV - REPRESENTATIONS AND INSTRUCTIONS**	
X	E	INSPECTION AND ACCEPTANCE	73		K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
X	F	DELIVERIES OR PERFORMANCE	74				
X	G	CONTRACT ADMINISTRATION DATA	75 - 77		L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
X	H	SPECIAL CONTRACT REQUIREMENTS	78 - 81		M	EVALUATION FACTORS FOR AWARD	

OFFER (Must be fully completed by offeror)

NOTE: Item 12 does not apply if the solicitation includes the provisions at 52.214-16, Minimum Bid Acceptance Period.

12. In compliance with the above, the undersigned agrees, if this offer is accepted within _____ calendar days (60 calendar days unless a different period is inserted by the offeror) from the date for receipt of offers specified above, to furnish any or all items upon which prices are offered at the price set opposite each item, delivered at the designated point(s), within the time specified in the schedule.

13. DISCOUNT FOR PROMPT PAYMENT (See Section I, Clause No. 52.232-8)	

14. ACKNOWLEDGMENT OF AMENDMENTS (The offeror acknowledges receipt of amendments to the SOLICITATION for offerors and related documents numbered and dated):	AMENDMENT NO.	DATE	AMENDMENT NO.	DATE

15A. NAME AND ADDRESS OF OFFEROR	CODE	FACILITY	16. NAME AND TITLE OF PERSON AUTHORIZED TO SIGN OFFER (Type or print)
PRAESCIENT ANALYTICS LLC GOVERNMENT REPRESENTATIVE 635 SLATERS LN STE 200 ALEXANDRIA VA 22314-1109	6HK06		

15B. TELEPHONE NO (Include area code)	15C. CHECK IF REMITTANCE ADDRESS IS DIFFERENT FROM ABOVE - ENTER SUCH ADDRESS IN SCHEDULE.	17. SIGNATURE	18. OFFER DATE
(703)739-2110	☐		

AWARD (To be completed by Government)

19. ACCEPTED AS TO ITEMS NUMBERED	20. AMOUNT	21. ACCOUNTING AND APPROPRIATION
0001 through 0012	$45,279,088.71	

22. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:	23. SUBMIT INVOICES TO ADDRESS SHOWN IN (4 copies unless otherwise specified)	ITEM
☐ 10 U.S.C. 2304(c)( ) ☐ 41 U.S.C. 253(c)( )	1	Section G

24. ADMINISTERED BY (If other than Item 7)	CODE	25. PAYMENT WILL BE MADE BY	CODE
DCMA MANASSAS 14501 GEORGE CARTER WAY CHANTILLY VA 20151 SCD: B	S2404A	DFAS COLUMBUS CENTER DFAS-CO/SOUTH ENTITLEMENT OPS P.O. BOX 182264 COLUMBUS OH 43218-2264	HQ0338

26. NAME OF CONTRACTING OFFICER (Type or print)	27. UNITED STATES OF AMERICA	28. AWARD DATE
DANIEL K. VOLA TEL: 843-218-2500 EMAIL: daniel.vola@navy.mil	(b)(6) (Signature of Contracting Officer)	26-Oct-2018

IMPORTANT - Award will be made on this Form, or on Standard Form 26, or by other authorized official written notice.

Section A - Solicitation/Contract Form

NOTE:

This contract award includes the offeror's proposal in response to solicitation number N65236-16-R-0001 and the offeror's acknowledgement of amendments 0001 through 0005, as follows:

Amendment No.	Date
0001	5/10/2017
0002	5/11/2017
0003	5/18/2017
0004	6/22/2017
0005	2/16/2018

Section B - Supplies or Services and Prices

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0001		1	Each	(b)(4)	(b)(4)

Advanced Analytics Technical SolutionFFP
Delivery of Advanced Analytics Technical Solution (AATS) Software, including Software Updates and Security Updates for a period of one year, in accordance with the Performance Work Statement
FOB: Destination
PSC CD: 7030

MAX NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0002		1	Lot		NSP

Advanced Analytics Technical SolutionFFP
Delivery of AATS Software Documentation/Technical Data Package in accordance with Performance Work Statement
Price for CLIN 0002 is included in the price for CLIN 0001
FOB: Destination
PSC CD: 7030

MAX NET AMT

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0003		1	Lot		NSP

Advanced Analytics Technical SolutionFFP
Delivery of AATS Systems Approach Training (SAT) Materials in accordance with Performance Work Statement

Price for CLIN 0003 is included in the price for CLIN 0001FOB: Destination
PSC CD: 7030

MAX
NET AMT

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0004		1	Lot	(b)(4)	(b)(4) NTE

Advanced Analytics Technical SolutionFFP-LOE
Original Equipment Manufacturer (OEM) / Subject Matter Expert (SME) Support Services for AATS Integration, Configuration, System Administration, Test, and IA in accordance with the Performance Work Statement.

In the performance of CLIN 0004 of this contract, the contractor shall provide the following estimated level of effort at the proposed composite rates per hour by contract year:

Year 1
Estimated Level of Effort Composite Rate Per Hour
(b)(4) hours (b)(4)

Year 2
Estimated Level of Effort Composite Rate Per Hour
(b)(4) hours (b)(4)

Year 3
Estimated Level of Effort Composite Rate Per Hour
(b)(4) hours (b)(4)

Year 4
Estimated Level of Effort Composite Rate Per Hour
(b)(4) hours (b)(4)

Year 5
Estimated Level of Effort Composite Rate Per Hour
(b)(4) hours (b)(4)

All Years
Max Quantity Max Amount
(b)(4) hours (b)(4)

In accordance with FAR 16.207-2, entitlement to full payment is based on the determination by the Government that the required level of effort and reports have been provided and are acceptable.

FOB: Destination
PSC CD: 7030

MAX NET AMT	(b)(4)
CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0005	Advanced Analytics Technical SolutionFFP Sustainment for AATS Software Delivered Under CLIN 0001 - Increment 1, including Software Updates and Security Updates in accordance with the Performance Work Statement FOB: Destination PSC CD: 7030	1	Lot	(b)(4)	(b)(4)

MAX NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0006	Advanced Analytics Technical SolutionFFP Sustainment for AATS Software Delivered Under CLIN 0001 - Increment 2, including Software Updates and Security Updates in accordance with the Performance Work StatementFOB: Destination PSC CD: 7030	1	Lot	(b)(4)	(b)(4)

MAX NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0007		1	Lot	(b)(4)	(b)(4)
	Advanced Analytics Technical SolutionFFP Sustainment for AATS Software Delivered Under CLIN 0001 - Increment 3, including Software Updates and Security Updates in accordance with the Performance Work Statement FOB: Destination PSC CD: 7030				

MAX NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0008		1	Lot	(b)(4)	(b)(4)
	Advanced Analytics Technical SolutionFFP Sustainment for AATS Software Delivered Under CLIN 0001 - Increment 4, including Software Updates and Security Updates in accordance with the Performance Work Statement FOB: Destination PSC CD: 7030				

MAX NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0009		1	Lot	(b)(4)	(b)(4)

Advanced Analytics Technical SolutionFFP-LOE
AATS Pre-Planned Product Improvements in accordance with the Performance Work Statement

In the performance of CLIN 0009 of this contract, the contractor shall provide the following estimated level of effort at the proposed composite rates per hour by contract year:

Year 2
Estimated Level of Effort Composite Rate Per Hour
(b)(4) hours (b)(4)

Year 3
Estimated Level of Effort Composite Rate Per Hour
(b)(4) hours (b)(4)

Year 4
Estimated Level of Effort Composite Rate Per Hour
(b)(4) hours (b)(4)

Year 5
Estimated Level of Effort Composite Rate Per Hour
(b)(4) hours (b)(4)

All Years
Max Quantity Max Amount
(b)(4) hours (b)(4)

In accordance with FAR 16.207-2, entitlement to full payment is based on the determination by the Government that the required level of effort and reports have been provided and are acceptable.
FOB: Destination
PSC CD: 7030

MAX NET AMT	(b)(4)
CEILING PRICE	$0.00

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0010		UNDEFINED			NSP

CDRLsFFP
Contract Data Requirements List (CDRLs) in accordance with Performance Work Statement - Not Separately Priced

MAX NET AMT $0.00

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0011		14	Lot	(b)(4)	(b)(4)

Advanced Analytics Technical SolutionFFP
Contract Years 2 Through 5 - Additional AATS Software Licenses/User Capacity, including License Agreement, License Renewals, Software Updates, and Security Updates For Additional AATS Software Users Through End of Contract Performance Period, in accordance with the Performance Work Statement
Note - Additional AATS Software Licenses/User Capacity Will Be Purchased in Lots of 100, where 1 Lot is equal to 100 Additional Concurrent UsersFOB: Destination
PSC CD: 7030

MAX NET AMT (b)(4)

ITEM NO	SUPPLIES/SERVICES	MAX QUANTITY	UNIT	UNIT PRICE	MAX AMOUNT
0012		1	Lot	(b)(4)	(b)(4) NTE

Travel and Other Direct CostsFFP
The contractor shall perform in accordance with PWS paragraph 14.0. Not-To-Exceed (b)(4). Specific requirements will be priced at the task order level.FOB: Destination
PSC CD: 7030

MAX NET AMT	$294,824.61

CLAUSES INCORPORATED BY FULL TEXT

5252.216-9218 MINIMUM AND MAXIMUM QUANTITIES (JUL 1989)

As referred to in paragraph (b) of the "Indefinite Quantity" clause of this contract, the contract minimum quantity is a total of $25,000 worth of orders at the contract unit price(s). The contract minimum quantity will be satisfied via the issuance of Delivery Order 0001, which will be issued concurrently with contract award (see solicitation Attachment 13 – Delivery Order 0001 Statement of Work). The maximum quantity is the total estimated amount of the contract. The maximum quantity is not to be exceeded without prior approval of the Procuring Contracting Officer.

(End of clause)

Section C - Descriptions and Specifications

SPECIFICATIONS/WORK STATEMENT
Work under this performance-based contract shall be performed in accordance with the following description/ specifications/ statement of work (SOW) which herein shall be referred to as Performance Work Statement (PWS):

1.0 PURPOSE

1.1 BACKGROUND

The Space and Naval Warfare Systems Center (SPAWARSYSCEN) Atlantic, Expeditionary Intelligence Solutions (EIS) Portfolio, Distributed Common Ground Surface/System (DCGS) Marine Corps Integrated Product Team, Intelligence Analysis System (IAS) program supports the United States Marine Corps (USMC) all-source intelligence analyst (Military Occupational Specialty (MOS) 0231) in the processing, exploitation, analysis, interpretation, and presentation of all-source intelligence data. The IAS Family of Systems (IAS FoS) provides support to multiple echelons, from the Marine Expeditionary Force (MEF) to the Company level, through the employment of intelligence servers and workstations. The Intelligence Server – Windows (IS-W) is a physical server with VMWare ESXi hypervisor installed, and hosts multiple virtual machines that provide collaboration, track management, and common operational picture (COP) services for the intelligence analyst, and provides access to Global Command and Control System – Joint (GCCS-J) and GCCS- Integrated Intelligence and Imagery (GCCS-I3) services. The IS-W is deployed at all levels of the Marine Air Ground Task Force (MAGTF) down to the regimental echelon and Marine Expeditionary Units (MEU). Intelligence Workstations (IW) are present at all echelons of the MAGTF down to the Company level, can utilize services on the IS-W (Modernized Integrated Database (MIDB), COP, chat, etc.), and can also operate in standalone mode.

Advancements in the technology fields of knowledge management and data science present opportunities to introduce efficiencies in the intelligence cycle (Marine Corps Doctrinal Publication (MCDP 2-1) through utilization of ontologies to structure data from disparate sources as well as integration of predictive analytics, natural language processing, and related technologies; and the use of emerging and non-traditional database technologies and architectures to support the efficient search and retrieval of information. Therefore, the IAS program has initiated an Advanced Analytics Technical Solution (AATS) project to identify and acquire an enterprise-capable software solution that supports the activities and intent of each phase of the intelligence cycle, reduces manual effort through application of advanced analytics technologies, and functions in both connected and disconnected modes of operation. “Enterprise-capable” software solution means the software must provide capability that scales to the available computing resources at each echelon. “Connected and disconnected modes of operation” primarily refers to the ability of the IW to communicate with the IS-W over the network. It can also refer to the connectivity of the IW and the IS-W to the Marine Corps Enterprise Network (MCEN).

1.2 SCOPE

The scope of this PWS includes the procurement of an advanced analytics software product, using commercial item (CI) or non-developmental item (NDI) components (see Federal Acquisition Regulation 2.101 for the definition of commercial item and non-developmental item) to the maximum extent practicable, that will 1) assist with the processing, exploitation, analysis, interpretation, and presentation of all-source intelligence data; and 2) include a robust, open application programming interface (API) that provides extensive support for integration of Government-developed and commercially-developed application plugins and integration between AATS data storage and external data sources. The software will minimize total ownership costs, and will accommodate the characteristics of the user population that will operate, maintain, and support the software without support from Field Service Representatives (FSRs) and the key missions, operations, and decisions that the software must support.

The scope of this PWS may include non-commercial development that is layered over the CI or NDI components. The development of this layer will allow for a more a robust, open application programming interface (API) that provides extensive support for integration of Government-developed and commercially-developed application plugins and integration between AATS data storage and external data sources, both the IS-W and at the IW’s. The non-commercial development, when combined with the APIs will allow for a modular open software environment,

which can support substitution of either commercial products or the non-commercial layer, on either side of the API, and at both the IS-W and at the IW.

The scope also includes the services required to support SPAWARSYSCEN Atlantic personnel in the engineering, integration, information assurance, testing, and training activities required for the program to deploy the software to the MEF within the IAS architecture; and to ensure that SPAWARSYSCEN Atlantic personnel can maintain the software on the IAS baseline without additional vendor support. The Program Sponsor is the Marine Corps Systems Command (MARCORSYSCOM).

The AATS software shall support the following tiered IAS FoS composition:

- IAS-FoS, Tier I (10 fielded systems, two stacks per system): The Tier I of the IAS FoS is the MEF IAS which supports the MEF Command Element in garrison and deployed.
- IAS-FoS, Tier II (132 fielded systems, one stack per system): The Tier II of the IAS FoS is made up of IS-W systems which are cased into transportable server suites. The Tier II supports the Marine Divisions, Marine Aircraft Wings, Marine Logistics Groups, Intelligence Battalions, Marine Expeditionary Units, infantry and artillery regiments, and air groups.
- IAS-FoS, Tier III (2574 fielded systems): The Tier III of the IAS FoS is made up of Intelligence Workstations which are man-portable, Windows-based systems that support battalions, squadrons, companies, and select higher echelon headquarters.

NOTE: Work will not be performed in Afghanistan.

2.0 APPLICABLE DOCUMENTS (AND DEFINITIONS)

2.1 REQUIRED DOCUMENTS

The following instructional documents are mandatory for use during contract performance. Unless otherwise specified, the document's effective date of issue is the date on the request for proposal. Additional applicable documents may be included in specific task orders.

	Document Number	Title
a.	DoD 5200.2-R	DoD Regulation – Personnel Security Program, dtd Jan 87
b.	DoDM 5200.01	DoD Manual – Information Security Program Manual, dtd 24 Feb 12
c.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program, dtd 20 Jun 12
d.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual, dtd 3 Nov 08
e.	DoD 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM), dtd 28 Feb 06
f.	DoDI 5220.22	DoD Instruction – National Industrial Security Program, dtd 18 Mar 11
g.	DoDI 6205.4	Department of Defense Instruction, Immunization of Other Than U.S. Forces (OTUSF) for Biological Warfare Defense, dtd 14 Apr 00
h.	DoDI 8500.01	DoD Instruction – Cybersecurity, dtd 14 Mar 14
i.	DoDI 8510.01	DoD Instruction – Risk Management Framework (RMF) for DoD Information Technology (IT), dtd 12 Mar 14
j.	DoD 8570.01-M	Information Assurance Workforce Improvement Program, dtd 19 Dec 05 with Change 3, dtd 24 Jan 12
k.	DoDD 8570.01	DoD Directive – Information Assurance Training, Certification, and Workforce Management, dtd 15 Aug 04
l.	SECNAV M-5239.2	DON Information Assurance Workforce Management Manual, dtd May 2009

m.	SECNAV M-5510.30	Secretary of the Navy Manual – DoN Personnel Security Program, dtd Jun 2006
n.	SECNAVINST 5239.3B	DoN Information Assurance Policy, dtd 17 Jun 09
o.	SECNAVINST 5510.30B	DoN Regulation – Personnel Security Program, dtd 6 Oct 06
p.	SPAWARINST 3432.1	SPAWAR Instruction – Operations Security (OPSEC) Policy, dtd 2 Feb 05
q.	SPAWARINST 5721.1B	SPAWAR Section 508 Implementation Policy, dtd 17 Nov 09
r.	SPAWARSYSCENLANTINST 12910.1A	Space and Naval Warfare Systems Center Atlantic Instruction – Deployment of Personnel and Contractor Employees to Specific Mission Destinations, dtd 28 Dec 09
s.	Marine Corps Doctrinal Publication (MCDP) 2	Intelligence, dtd 7 Jun 97
t.	Marine Corps Warfighting Publication (MCWP) 2-10	Intelligence Operations, dtd 2 May 16
u.	Marine Corps Tactical Publication (MCTP) 2-10A	MAGTF Intelligence Collection, dtd 2 May 16
v.	Marine Corps Tactical Publication (MCTP) 2-10B	MAGTF Intelligence Production and Analysis, dtd 2 May 16

2.2 GUIDANCE DOCUMENTS

The following documents are to be used as guidance during contract performance. Unless otherwise specified, the document's effective date of issue is the date on the request for proposal. Additional applicable documents may be included in specific task orders.

	Document Number	**Title**
a.	MIL-STD-1916	DoD Test Method Standard – DoD Preferred Methods for Acceptance Of Product, dtd 01 Apr 96
b.	DoDI 3020.41	DoD Instruction – Operational Contract Support (OCS), dtd 20 Dec 10
c.	DoDD 5000.01	DoD Directive – The Defense Acquisition System, dtd 20 Nov 07
d.	DoDI 5000.02	DoD Instruction – Operation of the Defense Acquisition System, dtd 07 Jan 15
e.	ISO/IEC 12207	International Organization for Standardization/ International Electrotechnical Commission: Systems and Software Engineering – Software Life Cycle Processes
f.	ISO/IEC 15288	International Organization for Standardization/ International Electrotechnical Commission: Systems and Software Engineering – System Life Cycle Processes
g.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors, dtd 27 Aug 04
h.	DoDM-1000.13-M-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle, dtd 23 Jan 14
i.	FIPS PUB 201-2	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, dtd Aug 2013
j.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment

	Document Number	Title
		Eligibility Verification
i.	N/A	SPAWARSYSCEN Atlantic Contractor Check-in portal – https://wiki.spawar.navy.mil/confluence/display/SSCACOG/Contractor+Checkin
j.	N/A	SPAWARSYSCEN Atlantic OCONUS Travel Guide portal – https://wiki.spawar.navy.mil/confluence/display/SSCACOG/OCONUS+Travel+Guide
k.	NAVMC 1553.1	Systems Approach to Training User's Guide, dtd 27 Oct 10
l.	[N/A]	Marine Corps Systems Approach to Training Manual
m.	[N/A]	Defense Information Systems Agency (DISA) Security Requirements Guide (SRG)
n.	[N/A]	DISA Security Technical Implementation Guides (STIGs)
o.	[N/A]	OWL Web Ontology Language Document Overview
p.	[N/A[	OWL 2 Web Ontology Language XML Serialization (Second Edition) – W3C Recommendation, dtd 11 Dec 12
q.	IEEE Std 12207-2008	Systems and Software Engineering – Software Life Cycle Processes

2.3 SOURCE OF DOCUMENTS

The contractor shall obtain all applicable documents. Many documents are available from online sources. Specifications and commercial/industrial documents may be obtained from the following sources:

Copies of Federal Specifications may be obtained from General Services Administration Offices in Washington, DC, Seattle, San Francisco, Denver, Kansas City, MO., Chicago, Atlanta, New York, Boston, Dallas and Los Angeles.

Copies of military specifications may be obtained from the Commanding Officer, Naval Supply Depot, 3801 Tabor Avenue, Philadelphia, PA 19120-5099. Application for copies of other Military Documents should be addressed to Commanding Officer, Naval Publications and Forms Center, 5801 Tabor Ave., Philadelphia, PA 19120-5099.

All other commercial and industrial documents can be obtained through the respective organization's website.

3.0 PERFORMANCE REQUIREMENTS

The following paragraphs list all products and services that shall be required throughout the contract life. The contractor shall provide necessary resources and knowledge to support the listed supply and services requirements. Specific objectives will be dependent on the basic contract and the delivery/task order (TO) written against the basic contract. The contractor shall complete all required deliveries/tasks while controlling and tracking performance and goals in terms of price, schedules, and resources.

Note: In compliance with SPAWARINST 4720.1A – SPAWAR Modernization and Installation Policy, all contract installation work performed aboard Navy ships and Navy shore sites is under Installation Management Office (IMO) supervision; otherwise, a formal exemption request has been approved. In accordance with the Fleet Readiness Directorate Standard Operating Procedure (FRD SOP), COMSPAWARSYSCOM letter Ser FRD/235 dated 24 Apr 12, the contractor shall ensure proper notification and status updates of installation work performed outside of SPAWARSYSCEN Atlantic respective Areas of Responsibilities (AORs) are provided to the SPAWAR Officer in Charge (OIC) or applicable Geographic Lead.

3.1 Open Systems Approach

The AATS software product shall, to the maximum extent practicable, have an Open System Architecture and corresponding components. The contractor shall define, document, and follow an open systems approach for using modular design, standards-based interfaces, and widely-supported consensus-based standards. The contractor shall develop, maintain, and use an Open System Management Plan (CDRL A002) to support this approach and shall demonstrate compliance with that plan during all design reviews.

In satisfying the Government's requirements, the following system architecture approach characteristics shall be utilized:

3.1.1 Open Architecture

The contractor's AATS software product shall encompass an architecture that incorporates appropriate considerations for re-configurability, portability, maintainability, technology insertion, vendor independence, reusability, scalability, interoperability, upgradeability, and long-term supportability. The contractor architecture shall include well-defined interfaces that allow for substitution of components on either side of the interface.

The contractor shall ensure that external information exchange requirements are implemented in a standard and open manner as part of this effort. These actions shall include planning that identifies the contractor's specific approach to ensuring software and interface data is well-defined, available to all programs, and uses a standards-based tool for definition within the context of DoD and Service upgrade programs.

3.1.2 Modular, Open Design

The contractor shall provide an AATS software product with an architecture that is layered and modular and uses standards-based commercial item/NDI software, operating systems, and middleware that shall utilize either non-proprietary or non-vendor-unique key module or component interfaces where available. Any software components, applications or software or interface data that are developed under the contract will be considered non-commercial software that is developed at Government expense. The contractor's design approach shall be consistent throughout all subsystems and components.

Module Coupling – The contractor's design approach shall result in modules that have minimal dependencies on other modules (loose coupling), as evidenced by simple, well-defined interfaces and by the absence of implicit data sharing. The purpose is to ensure that any changes to one module will not necessitate extensive changes to other modules, and hence facilitate module replacement and system enhancement.

Module Cohesion – The contractor's design shall result in modules that are characterized by the singular assignment of identifiable and discrete functionality (high cohesion). The purpose is to ensure that any changes to system behavioral requirements can be accomplished by changing a minimum number of modules within the system.

System Requirements Accountability – The contractor shall ensure that all software requirements in this PWS are accounted for through a demonstrated ability to trace each requirement to one or more modules that consist of components that are self-contained elements with well-defined, open, and published interfaces implemented using open standards.

Inter-component Dependencies – The contractor's design approach shall result in a layered system design, maximizing software independence from the hardware, thereby facilitating technology refresh. The design shall be optimized at the lowest component level to minimize inter-component dependencies. The layered design shall also isolate the application software layers from the infrastructure software (such as the operating system) to enhance portability and to facilitate technology refresh. The design shall be able to survive a change to the computing infrastructure with minimal or no changes required to the application logic. The interfaces between the layers shall be built to open standards or the technical data describing the interface shall be available to the Government with at least Government Purpose Rights. The software architecture shall minimize inter-component dependencies to allow components to be decoupled and reused, where appropriate, across various DoD or Service programs and platforms.

3.1.3 Technology Insertion

The contractor's architectural approach shall support the rapid and affordable insertion and refreshment of technology through modular design, the use of open standards and open interfaces. The contractor shall define the functional partitioning and the logical modularity of the system software subsystems and components to facilitate future replacement of specific subsystems and components without impacting other parts of the system and to encourage third-party vendor's participation.

3.1.4 Life Cycle Management and Open Systems

The contractor's architecture shall provide for insertion of commercial items into the system and, as directed at the delivery order/task order level, (a) demonstrate that commercial item, reusable NDI, and other components are logistically supported throughout the life cycle, (b) describe and demonstrate the strategy for reducing product or system and associated supportability costs through insertion of commercial items and other reusable commercial item or NDI products, (c) establish a process to logistically support commercial item or NDI products, and (d) shall provide the proposed methodology for pass through of commercial item warranties to the Government.

3.1.5 Use of Standards

The contractor's architectural approach shall use the following standards in descending order of importance:

Standards as specified within the contract, including task orders.

Commercial standards:

Standards developed by international or national industry standards bodies that have been widely adopted by industry. Examples of widely adopted standards are:

SQL for databases (e.g., SQL for databases ANSI ISO/IEC 9075-1, ISO/IEC 9075-2, ISO/IEC 9075-3, ISO/IEC 9075-4, ISO/IEC 9075-5)

HTML for presentation layer (e.g., XML 1.0 www.webstandards.org)

JSON for data transfer

Web services for remote system calls

Standards adopted by industry consensus-based standard bodies and widely adopted in the market place.

De facto standards (those widely adopted and supported in the market place).

Note: Standards that are not specified within this contract or that are modified shall be submitted to and approved by the Government Program Manager prior to use.

3.1.6 Life Cycle Sustainability

The contractor shall consider use of commercial items/NDI and open standards to enhance the system's life cycle sustainability by implementing performance-based logistics (PBL) arrangements to sustain the components through their life cycle.

3.1.7 Interface Design and Management

The contractor shall:

Clearly define, identify and describe all component and system interfaces;

Define and document all subsystem and configuration item (CI) level interfaces to provide full functional, logical, and physical specifications;

Identify the interface and data exchange standards between the component, module or system and the interconnectivity or underlying information exchange medium;

Use the identified interfaces to support an overall information assurance strategy that implements Information Assurance (IA) Processes in accordance with DoD Instruction 8500.2 (dated February 6, 2003) and;

If applicable, select external interfaces from existing open or Government standards with an emphasis on enterprise-level interoperability. The contractor shall describe how its selection of interfaces will maximize the ability of the system to easily accommodate technology and facilitate the insertion of alternative or reusable modular system elements on either side of the interface.

3.1.8 Treatment of Proprietary or Vendor-Unique Elements

The contractor shall explain the use of proprietary, vendor-unique or closed components or interfaces. If applicable, the contractor shall define its process for identifying and justifying proprietary, vendor-unique or closed interfaces, code modules, hardware, firmware, or software to be used. When interfaces, hardware, firmware, or modules that are proprietary or vendor-unique are required, the contractor shall demonstrate to the Government that those proprietary elements do not preclude or hinder other component or module developers from interfacing with or otherwise developing, replacing, or upgrading open parts of the system.

3.2. SOFTWARE PERFORMANCE SPECIFICATION

Within 90 days after date of contract (ADC) and concurrent issuance of Delivery Order 0001, the contractor shall deliver an AATS software solution ready for functional integration into the IAS system baseline in accordance with the requirements of this section (CLIN 0001).

3.2.1 Technical Maturity (CLIN 0001)

The AATS software shall support the capabilities defined in this specification and its attachments, either out of the box or with configuration changes.

The components and modules of the proposed AATS software shall have been previously integrated and deployed together in a similar production environment as defined in this specification.

3.2.2 Software Compatibility (CLIN 0001)

Background

The Government will install and integrate the AATS software into the IAS system baseline, using the AATS documentation deliverables. The Government does not intend to introduce additional hardware into the IAS system baseline to support the system requirements of the AATS software. Therefore, the AATS software must function within the hardware and software constraints of the IAS system baseline at the time of award.

AATS Software Requirements

3.2.2.1 Vendor-specified system requirements for AATS software components installed on the IW shall not exceed the IW hardware and software specification (Solicitation Attachment 6).

3.2.2.2 Vendor-specified system requirements for AATS software components installed on the IS-W shall not exceed the IS-W hardware and software specification (Solicitation Attachment 6).

3.2.2.3 AATS software components installed on the IS-W shall be capable of operating in Virtual Machines (VMs) managed by VMWare ESXi hypervisor software.

3.2.2.4 AATS software components installed on the IS-W shall be compatible with Microsoft Server 2012 Operating System or Red Hat Linux 7.

3.2.2.5 AATS software components installed on the IW shall be compatible with Microsoft Windows 10 Operating System.

3.2.2.6 AATS software components that require the use of a web browser shall be fully compatible with the web browser software versions listed in the IS-W and IW software specification (Solicitation Attachment 6). Updates to the AATS software components shall be provided to maintain compatibility with updates to the web browser software on the IS-W and IW software baselines.

3.2.3 Information Assurance (CLIN 0001)

The AATS software shall be compliant with all applicable Defense Information Systems Agency (DISA) information assurance requirements as provided in DISA Security Requirement Guides (SRGs) and Security Technical Implementation Guides (STIGs). The AATS software shall be able to be registered in the Department of the Navy Application and Database Management System (DADMS) and receive approval by the USMC Functional Area Manager (FAM).

3.2.4 Supportability

3.2.4.1 Once fielded as part of the IAS software baseline to the end users, the AATS software and all functionality provided by the AATS software shall be capable of being maintained without on-site contractor support. (CLIN 0001)

3.2.4.2 The contractor shall provide any and all AATS software version upgrades as they are released and no less than semiannually. (CLINs 0001, 0005, 0006, 0007, 0008, and 0011)

3.2.4.3 Upon notification of a security vulnerability in the AATS software or its dependencies, the contractor shall provide a fix or mitigation strategy according to the following timetable (CLIN 0005, 0006, 0007, 0008, and 0011):

Severity	Timeline for Response
Category I	72 hours
Category II	5 days
Category III	10 days

3.2.4.4 All AATS software version upgrades shall support non-destructive updates of the IAS software baseline. Software requirements that support non-destructive updates include, but are not limited to (CLIN 0005, 0006, 0007, 0008, and 0011):

All software package version upgrades shall support silent installation (installation with no user interaction required).

All software package version upgrades shall support scripted installation, where all installation parameters are accessible at the command line.

3.2.5 Functional Requirements (CLIN 0001)

3.2.5.1 Database and Ontology

Background/Definitions

In order to promote data consistency and interoperability between organizationally and/or geographically disparate USMC intelligence teams, and to provide a framework for the development of advanced analytical capabilities, the AATS software will conform all processed data to a Government-provided AATS ontology. "Processed data" means structured, semi-structured, and unstructured data from external sources that has been mapped to objects, relationships, and properties defined by the ontology. The standard form of the Government-provided ontology will be the XML/RDF serialization defined by the W3C OWL 2 Web Ontology Language XML Serialization (Second Edition).

The following definitions will be used for the AATS software requirements:

An Object Type is an abstract concept; for example, "Person", "Equipment", "Event", and "Facility".

An Object is an instance of an Object Type. Using the "Person" Object Type example, the user may create Objects from the "Person" Object Type that represent specific people (e.g. "John Doe").

A Relationship Type is an abstract relation where the domain and range are Object Types. For example:

Relationship Type ID: "is-located-at"
Domain: "Person", "Equipment"
Range: "Facility"

A Relationship is an instance of a Relationship Type (in the same way that an Object is an instance of an Object Type). Continuing the "is-located-at" Relationship Type example, the following are examples of valid Relationships:

"John Doe" (Person Object) "is-located-at" (Relationship) "Building XYZ" (Facility Object)

A Property Type is a specification of an attribute and its range of valid values. Some examples:

Height: positive integer

Body Style: "Sedan", "Coupe", "Truck"

Name: Unicode string

Property Types will be incorporated into the specification of one or more Object Types and Relationship Types. As part of the specification, Object Types and Relationship Types will identify additional constraints such as cardinality, required/not required, etc. For example:

Object Type: Person
- Property Type: "Name"
  - ID: "First Name"
  - Cardinality: 1
  - Required: True
- Property Type: "Name"
  - ID: "Last name"
  - Cardinality: 1
  - Required: True
- Property Type: "Name"
  - ID: "Alias"
  - Cardinality: Unbounded
  - Required: False

A Property is an instance of a Property Type in an Object or Relationship. Using the "Person" Object Type specification above, a valid Object could be:

Object ID: "John Doe"
Property ID: "First Name"
Value: "John"
Property ID: "Last Name"
Value: "Doe"
Property ID: "Alias"
Value: "Jack Deer"

AATS Software Requirements

3.2.5.1.1 The software shall include a database that supports the storage, management, and retrieval of Objects, Relationships, and Properties as defined by the Government-provided AATS ontology.

3.2.5.1.2 The software shall import and export the Government-provided AATS ontology in Web Ontology Language (OWL) 2 compliant RDF/XML format.

The contractor shall provide the Government with all ontology implementation requirements necessary to provide the capability defined in this specification (CDRL A002).

If the contractor requires that the Government-provided AATS ontology include or import XML schemas or ontologies, the contractor shall provide an electronic copy of the required documents (CDRL A002).

The combination of the Government-provided AATS ontology and any modifications to the Government-provided AATS ontology required by the contractor's ontology implementation requirements and/or contractor-provided XML schemas or ontologies shall result in an OWL 2 compliant RDF/XML ontology.

The ontology implementation requirements shall not restrict the ability of the Government to define direct subclasses of the OWL 2 Class "owl:Thing".

3.2.5.1.3 The software shall provide the capability to create new ontologies.

3.2.5.1.4 The software shall allow the combination of multiple ontologies so as to construct the overall ontology.

3.2.5.1.5 The software shall provide the capability to update the ontology, both via the software user interface and via the import of an updated Government-provided AATS ontology.

3.2.5.1.6 Prior to committing ontology changes, the software shall provide the capability to map existing data to the new ontology without data loss.

If the software is unable to map existing data to the new ontology without data loss, the software shall provide a report that identifies the data that will be lost as a result of the ontology update.

3.2.5.1.7 Prior to committing ontology changes, the software shall provide the capability to update mappings between data sources and data element mappings (see Section 3.2.5.2.3.3)

3.2.5.1.8 The software shall provide the capability to deploy the ontology to other instances of the AATS database.

3.2.5.1.9 The software shall provide the capability to visualize the ontology.

3.2.5.1.10 The software shall ensure that all data stored in the database is validated against the ontology.

The software shall support the use of Relationship Properties as defined in the Government-provided AATS ontology.

The software shall support the use of required Properties for Objects and Relationships as defined in the Government-provided AATS ontology.

3.2.5.1.11 The software shall support the Object Type taxonomy defined in the Government-provided AATS ontology.

3.2.5.1.12 The software shall support the Relationship Type taxonomy defined in the Government-provided AATS ontology.

3.2.5.1.13 The software shall provide the capability to deprecate Object Types such that no new Objects of that type can be created, and existing Objects of that type can be used in the search and analysis capabilities of the software.

3.2.5.2 Data Entry

Background

The processing and exploitation phase of the intelligence cycle involves the conversion of structured, semi-structured, and unstructured data into information that is suitable for the production of intelligence to satisfy intelligence requirements. The AATS software will provide manual, assisted, and automated data entry capabilities to support this phase of the intelligence cycle.

AATS Software Requirements

The software shall support the processing of structured, semi-structured, and unstructured data into Objects, Relationships, and Properties conformant with the Government-provided AATS ontology.

3.2.5.2.1 Manual Data Entry

3.2.5.2.1.1 The software shall allow the user to create and update Objects.

3.2.5.2.1.2 The software shall allow the user to set and update Property values for an Object.

3.2.5.2.1.3 When Property values for an Object are updated, the software shall preserve the history and attribution of changes to the Property value.

3.2.5.2.1.4 The software shall allow the user to create and update Relationships between Objects.

3.2.5.2.1.5 The software shall allow the user to archive Relationships between Objects.

3.2.5.2.1.6 The software shall allow the user to set and update Property values for a Relationship.

3.2.5.2.1.7 When Property values for a Relationship are updated, the software shall maintain the history and attribution of changes to the Property value.

3.2.5.2.1.8 The software shall allow the user to attach files to an Object.

3.2.5.2.1.9 The software shall allow the user to link an attachment to a specific Property.

3.2.5.2.1.10 The software shall allow the user to define a default image per Object Type.

3.2.5.2.1.11 The software shall allow the user to set a custom image per Object.

3.2.5.2.1.12 The software shall allow the user to define a default MIL-STD-2525D symbol for an Object Type.

3.2.5.2.1.13 The software shall allow the user to set the MIL-STD-2525D symbol for an Object.

3.2.5.2.1.14 The software shall allow the user to archive Objects. The archive operation shall archive the Relationships, Properties, and attachments for each archived Object.

3.2.5.2.1.15 The software shall allow the user to restore archived Objects.

3.2.5.2.1.16 The software shall exclude archived data from user searches unless the user specifies that archived data should be included in the search results.

3.2.5.2.1.17 The software shall exclude archived data from replication unless the user requests the inclusion of archived data.

3.2.5.2.1.18 The software shall allow the user to merge Objects.

3.2.5.2.1.19 The software shall allow the user to merge Relationships.

3.2.5.2.1.20 The software shall allow the user to assign a confidence value for the Object and the Properties for the Object.

3.2.5.2.1.21 The software shall allow the user to update the confidence value for the Object and the Properties for the Object.

3.2.5.2.1.22 The software shall allow the user to assign a confidence value for a Relationship and the Properties for the Relationship.

3.2.5.2.1.23 The software shall allow the user to update the confidence value for a Relationship and the Properties for the Relationship.

3.2.5.2.1.24 All Objects shall be labeled in accordance with (IAW) Intelligence Community Information Security Markings Metadata (ICISM) standards

3.2.5.2.1.25 All Relationships shall be labeled IAW ICISM standards.

3.2.5.2.1.26 All Property values shall be labeled IAW ICISM standards.

3.2.5.2.1.27 The classification for the Object should be equal to the highest Property value classification for the Object.

3.2.5.2.2 Tagging

Background

The tagging capability assists the user in creating structured data from unstructured or semi-structured documents. The user is able to identify and select Objects and Relationships in a document, and the AATS software identifies potential matches to those Objects in the AATS database. Via the tagging process, the user is able to associate the selected Object or Relationship to the AATS-identified match, or is able to create a new Object or Relationship from the selection that will be stored in the AATS database.

AATS Software Requirements

3.2.5.2.2.1 The software shall allow the user to tag Objects in documents.

3.2.5.2.2.2 The software shall allow the user to tag Relationships in documents.

3.2.5.2.2.3 The software shall identify to the user potential matches between tagged items and existing Objects and Relationships in the database.

The software shall allow the user to view and edit matches to tagged items.

3.2.5.2.2.4 The software shall allow the user to create Objects or Relationships from tagged items.

3.2.5.2.3 Automated Ingest

Background

The automated ingest capability provides for unattended conversion of intelligence data and information into Objects and Relationships. Data sources for the automated ingest capability include local and networked file storage, external databases, and web services. Data formats include documents, spreadsheets, and presentations, geospatial data files, United States Message Text Format (USMTF) messages, and other domain-specific formats. Objects and Relationships that are created by the software as a result of automated ingest will identify the source of the data, a reference to the data source (typically a Uniform Resource Indicator), and will maintain a copy of the data that was used to create the Object or Relationship. File content will be fully indexed to enable searching within documents via the search/query user interface.

AATS Software Requirements

3.2.5.2.3.1 The software shall provide the capability to ingest structured and semi-structured data from local and networked file storage, external databases, and web services.

3.2.5.2.3.2 The software shall provide the capability to map data elements from structured and semi-structured data sources to Objects, Relationships, and Properties.

3.2.5.2.3.3 The software shall provide the capability to associate data element mappings with specific data sources.

3.2.5.2.3.4 The software shall provide the capability to configure and execute a schedule for ingest of structured and semi-structured data.

3.2.5.2.3.5 The software shall allow the user to specify a local file source for automated ingest.

3.2.5.2.3.6 The software shall monitor specified file sources and automatically ingest new and modified files.

3.2.5.2.3.7 The software shall process all ingested files for Object and Relationship extraction.

The software shall identify Objects and Object Properties in processed files.

The software shall identify Relationships and Relationship Properties in processed files.

3.2.5.2.3.8 All ingested data shall retain the reference to the source of the data.

3.2.5.2.3.9 The software shall retain a source copy of the ingested data.

3.2.5.2.3.10 The software shall provide a capability to ingest data from the following file types:

Keyhole Markup Language (KML)
Shape files
Microsoft Office 2003 and later documents
Microsoft Office 2003 and later spreadsheets
Microsoft Office 2003 and later presentations
Portable Document Format (PDF)
Text files
Rich Text files (RTF)
Comma separated value (CSV)
National Imagery Transmission Format (NITF)
Tagged Image File Format (TIFF)
Geospatial Tagged Image File Format (GEOTIFF)
Joint Photographic Experts Group (JPEG)
JPEG 2000 (JP2) files
Portable Network Graphics (PNG)
Windows Metafile (WMF)
Compressed Image Base (CIB)
North American Treaty Organization (NATO) Secondary Imagery Formats (NISF)

3.2.5.2.3.11 The software shall prevent duplicate files from being ingested.

3.2.5.2.3.12 The software shall automatically transform invalid Property values entries into allowable values.

3.2.5.2.3.13 The software shall allow the user to map ingested raw data elements to the ontology.

3.2.5.2.3.14 The software shall allow the user to associate raw data element mapping to specific data sources.

3.2.5.2.3.15 The software shall provide for a review of all automatically transformed Property values prior to committing to the AATS database.

3.2.5.2.3.16 Automated Ingest Review Capability

Background

The software shall have multiple safeguards against the generation of erroneous data from malformed or poorly structured data sources. These safeguards shall include a “dry run” ingest capability that, when executed, shall alert the analyst to potential ingest problems within the data source. It shall also provide the ability to review all auto-generated Objects and Relationships prior to committing to the database. Until this review has been performed, auto-generated Objects and Relationships shall be searchable but clearly identified as “pending review.”

AATS Software Requirements

The software shall mark all automatically-identified Objects, Relationships, and Properties as “pending review”.

The software shall provide the analyst with the capability to review and approve or reject Objects, Relationships, and Properties that are “pending review”.

The software shall provide a dry run ingest capability that alerts the analyst to potential problems with the source data.

3.2.5.3 Map Display

3.2.5.3.1 The software shall provide a map display.

3.2.5.3.2 The map display shall be capable of retrieving map images utilizing the Open Geospatial Consortium (OGC) Web Map Service (WMS) Interface standard.

3.2.5.3.3 The map display shall provide the display of data and map layers, and allow the user to toggle the layers on or off for viewing.

3.2.5.3.4 The software shall be capable of displaying map data in the following formats:

Tactical Land Map (.tlm)
.TPC
Joint Operations Graphic (.jog)
Operations Navigational Chart (.onc)
City Graphic
.GNC
Joint Navigation Chart (.jnc)
Vector Map (.vmap)
Digital Terrain Elevation Map (.dted)
CIB
.SRTM
Interim Terrain Data (.itd)
Vector Interim Terrain Data (.vitd)
Raster Graphic
LIDAR

3.2.5.3.5 The software shall support the latitude and longitude, Military Grid Reference System (MGRS), and Universal Transverse Mercator (UTM) standard coordinate systems.

3.2.5.3.6 The map view shall support displaying Objects utilizing the defined image or symbol; or, if not available, the map view shall display the default image or symbol for an Object.

3.2.5.3.7 The map view shall be capable of displaying mensurated images.

3.2.5.4 Data Organization

Background

Operations, in the context of AATS, are a container for organizing data in support of intelligence analysis for a real-world operation. For example, “Operation Iraqi Freedom” could be a top-level container for data collected and included within the scope of the operation. Missions are similar to Operations on a smaller scale, but associated with an Operation (Operations have a one-to-many relationship to Missions). Finally, Area of Operations (AOs), Areas of Influence (AIs), Areas of Interest (AOIs), and Areas of Responsibility (AORs) are geospatially-based containers to organize data within an Operation or a Mission.

Note that data can be associated with multiple Operations, Missions, AOs, AIs, AOIs, and AORs – for example, hostile actors that support enemy forces in multiple Operations.

AATS Software Requirements

3.2.5.4.1 The software shall allow the user to create, view and update an operation.

3.2.5.4.2 The software shall allow the user to archive an operation.

3.2.5.4.3 The software shall allow the user to create, view and update missions.

3.2.5.4.4 The software shall allow the user to archive a mission.

3.2.5.4.5 The software shall allow the user to create, view and update an Area of Operations (AO) on a map.

3.2.5.4.6 The software shall allow the user to associate an AO to an operation.

3.2.5.4.7 The software shall allow the user to archive an AO and all associated data and files.

3.2.5.4.8 The software shall allow the user to create, view and update an Area of Influence (AI) on a map.

3.2.5.4.9 The software shall allow the user to associate an AI to an operation.

3.2.5.4.10 The software shall allow the user to archive an AI and all associated data and files.

3.2.5.4.11 The software shall allow the user to create, view and update an Area of Interest (AOI) on a map.

3.2.5.4.12 The software shall allow the user to associate an AOI to an operation.

3.2.5.4.13 The software shall allow the user to archive an AOI and all associated data and files.

3.2.5.4.14 The software shall allow the user to create, view and update an Area of Responsibility (AOR) on a map.

3.2.5.4.15 The software shall allow the user to associate an AOR to an operation.

3.2.5.4.16 The software shall allow the user to archive an AOR and all associated data and files.

3.2.5.5 Search

The software shall provide the user a search interface for conducting queries.

The software shall allow the user to save, retrieve, and execute queries.

The software shall allow the user create standing queries and the ability to convert saved queries to standing queries.

The software shall allow the user to define an alert based on standing queries.

The software shall notify the user, via the application user interface, when new data is available that matches a standing query.

The software shall notify the user, via the application user interface, when data associated with a standing query is modified or deleted.

Files processed by the data ingest capability shall be searchable via the search interface.

The software shall allow the user to query the full content of the files, including file metadata, via the search interface.

All Objects and Relationships shall be able to be queried via the search interface.

The software shall learn from user interaction with search results in order to improve relevance of search results.

3.2.5.5.1 Contextual Query

3.2.5.5.1.1 The software shall allow the user to conduct queries based on Property values and keywords.

3.2.5.5.1.2 The software shall allow the user to conduct queries based on Property values, multiple Property values, and keywords using ‘and’, ‘or’, and ‘not’ Boolean operators.

3.2.5.5.1.3 The software shall allow the user to conduct queries based on the exclusion of one or more Property values and keyword using ‘not’ Boolean operators.

3.2.5.5.1.4 The software shall attempt to automatically complete keywords entered in the contextual search field.

3.2.5.5.2 Geospatial Query

3.2.5.5.2.1 The software shall allow the user to conduct proximity queries relative to a point location.

3.2.5.5.2.2 The software shall allow the user to conduct proximity queries relative to multiple point locations using ‘AND’, ‘OR’, and ‘NOT’ Boolean operators.

3.2.5.5.2.3 The software shall allow the user to conduct proximity queries along a polyline.

3.2.5.5.2.4 The software shall allow the user to conduct proximity queries along multiple polylines using ‘AND’, ‘OR’, and ‘NOT’ Boolean operators.

3.2.5.5.2.5 The software shall allow the user to conduct proximity queries within a polygon.

3.2.5.5.2.6 The software shall allow the user to conduct proximity queries within multiple polygons using ‘AND’, ‘OR’, and ‘NOT’ Boolean operators.

3.2.5.5.2.7 The software shall allow the user to conduct proximity queries within one or more polygons and along polylines using ‘AND’, ‘OR’, and ‘NOT’ Boolean operators.

3.2.5.5.2.8 The software shall allow the user to conduct proximity queries relative to one or more point location along one or more polyline within one or more polygons using one or more combination of ‘AND’, ‘OR’, and ‘NOT’ Boolean operators.

3.2.5.5.2.9 The software shall allow the user to search based on specific geospatial boundaries as specified in a Shape file or KML file.

3.2.5.5.2.10 For all proximity queries, the software shall allow the user to define the proximity radius.

3.2.5.5.3 Temporal Query

3.2.5.5.3.1 The software shall allow the user to conduct temporal queries.

3.2.5.5.3.2 The software shall allow the user to specify the Date Time Group (DTG) range to perform the temporal query.

3.2.5.5.3.3 The software shall allow the user to filter search results based on a DTG range, location information, report type, Object Type, Relationship Type, and Property.

3.2.5.5.4 Faceted Search

3.2.5.5.4.1 The software shall provide an interactive summary of returned query results with Object Type names listed.

3.2.5.5.4.2 The software shall group and enumerate the query results by Object Type name.

3.2.5.5.4.3 The software shall allow the user to filter query results by selecting an Object Type name.

3.2.5.5.4.4 The software shall provide an interactive summary of returned query results with Property name listed.

3.2.5.5.4.5 The software shall group and enumerate the query results by Property name.

3.2.5.5.4.6 The software shall allow the user to filter query results by selecting a Property.

3.2.5.5.4.7 The software shall provide an interactive summary of returned query results with Relationship Type name listed.

3.2.5.5.4.8 The software shall group and enumerate the query results by Relationship Type name.

3.2.5.5.4.9 The software shall allow the user to filter query results by selecting a Relationship Type name.

3.2.5.6 Analysis

The software shall make recommendations to the user of Objects potentially related to an Object under user review, even if the recommended Objects do not have a defined relationship with the Object under user review.

3.2.5.6.1 Geospatial Analysis

3.2.5.6.1.1 The software shall allow the user to display Objects with geolocation data on a map.

3.2.5.6.1.2 The software shall support a line of sight analysis which depicts visibility from a given point on the ground.

3.2.5.6.1.3 The software shall support a terrain masking analysis which depicts visibility from a given point and altitude above ground.

3.2.5.6.2 Relationship Analysis

3.2.5.6.2.1 The software shall display Objects and Relationships in a link analysis view.

3.2.5.6.2.2 The software shall allow the user to display link analysis charts on a map

3.2.5.6.2.3 The software shall display Objects and Relationships in a social network analysis view.

3.2.5.6.2.4 The software shall display Objects and Relationships in an organizational hierarchy structure.

3.2.5.6.3 Charting

3.2.5.6.3.1 The software shall allow the user to conduct pattern analysis, trend analysis, and statistical analysis.

3.2.5.6.3.2 The software shall allow the user to generate column charts from Object and Property data.

3.2.5.6.3.3 The software shall allow the user to generate bar charts from Object and Property data.

3.2.5.6.3.4 The software shall allow the user to generate line charts from Object and Property data.

3.2.5.6.3.5 The software shall allow the user to generate pie charts from Object and Property data.

3.2.5.6.3.6 The software shall allow the user to generate area charts from Object and Property data.

3.2.5.6.3.7 The software shall allow the user to generate High-Low-Close charts from Object and Property data.

3.2.5.6.3.8 The software shall allow the user to generate scatter charts from Object and Property data.

3.2.5.6.3.9 The software shall allow the user to generate bubble charts from Object and Property data.

3.2.5.6.3.10 The software shall allow the user to generate radar charts from Object and Property data.

3.2.5.6.4 Temporal Analysis

3.2.5.6.4.1 The software shall allow the user to generate time wheel charts from Object and Property data.

3.2.5.6.4.2 The software shall allow the user to generate timeline charts from Object and Property data.

3.2.5.6.4.3 The software shall incorporate a time slider into the Map Display capability.

3.2.5.6.4.4 The software shall incorporate a time slider into the Relationship Analysis capability.

3.2.5.6.5 Heat Maps

The software shall allow the user to generate heat maps from Object and Property data and visualize on the Map Display capability.

3.2.5.7 Collaboration

Background

As part of the analytical process, users require a local workspace where products can be developed without altering the system data set (i.e. without altering the data seen by all users). The local workspace allows the users to create Objects and Relationships in the local workspace and to send Objects and Relationships from search actions into the local workspace. As the user works with these objects in the local workspace, all actions (create, update, delete) will only be seen within the workspace. In addition, when changes to objects are made outside of the workspace, the user will be notified and allowed to accept those changes into the workspace.

To promote collaboration and peer review, the software will allow the owner of the local workspace to share the local workspace with other selected users. Those selected users will have access to all of the workspace tools to create and modify the workspace Objects and Relationships. The software will provide a way for workspace collaborators to view changes and the user responsible for each change.

Finally, the software will allow the workspace owner to apply the workspace to the system data set. For example, if the workspace contains three modified Objects and two new Relationships, then applying the workspace to the system data set applies all of the modifications made to those Objects and creates the two new Relationships in the system data set.

AATS Software Requirements

3.2.5.7.1 The software shall allow the user to create a local view that is accessible only to the user that created the view.

3.2.5.7.2 The software shall allow the user to populate the local view with Objects and Relationships from the AATS database.

3.2.5.7.3 The software shall allow the user to create Objects in a local view.

3.2.5.7.4 The software shall allow the user to update Objects in a local view.

3.2.5.7.5 The software shall allow the user to remove Objects in a local view.

3.2.5.7.6 The software shall allow the user to create Relationships in a local view.

3.2.5.7.7 The software shall allow the user to update Relationships in a local view.

3.2.5.7.8 The software shall allow the user to remove Relationships in a local view.

3.2.5.7.9 The software shall allow the user to collaborate with selected users to share Objects and Relationships in a local view.

3.2.5.7.10 The software shall allow the user to promote Objects from the local view to the AATS database.

3.2.5.7.11 The software shall allow the user to promote Relationships from the local view to the AATS database.

3.2.5.7.12 The software shall notify the user when Objects or Relationships cannot be promoted due to conflicts with the system data.

3.2.5.7.13 The software shall assist the user in resolving conflicts between Objects or Relationships in the local view and Objects or Relationships in the system data.

3.2.5.8 Intelligence Journal

The software shall create a unique id for all entries logged in the integrated intelligence journal.

The integrated intelligence journal shall record the timestamp for all entries logged in the journal.

The integrated intelligence journal shall record the user or process, and the server location/ID for all entries logged in the journal.

The integrated intelligence journal shall record the timestamp at which all Objects are processed, created and updated.

Changes to document processing status shall be recorded in the integrated intelligence journal.

The approval of automatically extracted Objects or Relationships shall be logged in the integrated intelligence journal.

The manual extraction of Objects or Relationships shall be logged in the integrated intelligence journal.

The integrated intelligence journal shall log database replication events and the sending and receipt of all messages and reports.

The integrated intelligence journal shall allow the user to manually insert log entries that will be visually recognizable as having been manually entered.

The integrated intelligence journal shall allow the user to manually insert a comment on any automatically logged actions.

3.2.5.8.1 Search/Filter Intelligence Journal

3.2.5.8.1.1 The software shall allow the user to conduct contextual searches of the integrated intelligence journal.

3.2.5.8.1.2 The software shall allow the user to filter the integrated intelligence journal to find journal entries associated with an Operation.

3.2.5.8.1.3 The software shall allow the user to filter the integrated intelligence journal to find journal entries associated with a Mission.

3.2.5.8.1.4 The software shall allow the user to filter the integrated intelligence journal to find journal entries processed by a specific server location/ID.

3.2.5.8.1.5 The software shall allow the user to filter the integrated intelligence journal to find journal entries processed within a specific DTG range.

3.2.5.8.1.6 The software shall allow the user to filter the integrated intelligence journal to find journal entries containing a keyword(s).

3.2.5.8.1.7 The software shall allow the user to save filter settings.

3.2.5.8.1.8 The software shall allow the user to load previously saved filters.

3.2.5.8.2 Archive Intelligence Journal

3.2.5.8.2.1 The software shall allow the user to archive the integrated intelligence journal entries associated with a Mission.

3.2.5.8.2.2 The software shall allow the user to archive the integrated intelligence journal entries associated with an Operation.

3.2.5.8.2.3 The software shall allow the user to archive the integrated intelligence journal entries processed within a specific DTG range.

3.2.5.8.2.4 The software shall allow the user to recall archived journal entries.

3.2.5.8.3 Print Logged Data

The software shall allow the user to print the integrated intelligence journal.

3.2.5.8.4 Export Logged Data

The software shall allow the user to export the integrated intelligence journal to .xls.

3.2.5.9 Production

3.2.5.9.1 Graphics

3.2.5.9.1.1 The software shall be capable of creating and updating graphics.

3.2.5.9.1.2 The software shall be capable of reading graphics.

3.2.5.9.1.3 The software shall be capable of deleting graphics.

3.2.5.9.2 Overlays

3.2.5.9.2.1 The software shall be capable of creating and updating overlays.

3.2.5.9.2.2 The software shall be capable of displaying overlays on a map.

3.2.5.9.2.3 The software shall be capable of deleting overlays.

3.2.5.9.2.4 The software shall support overlays depicting Object data, MIL-STD-2525D symbology, shapes and lines of OGC standards, text, and images.

3.2.5.9.3 Reports

3.2.5.9.3.1 The software shall allow the user to create report templates.

3.2.5.9.3.2 The software shall allow the user to send query results to a report template.

3.2.5.9.3.3 The software shall allow the user to create reports utilizing report template.

3.2.5.9.3.4 The software shall allow the user to export Object data to .pptx, .docx, .xlsx, and .pdf formats.

3.2.5.9.3.5 The software shall allow the user to export charts and visualizations to .pptx, .docx, .xlsx, and .pdf formats.

3.2.5.9.4 Produce Tracks

The software shall be capable of producing unit tracks, acoustic tracks, platform tracks and Electronic Intelligence (ELINT) IAW MIL-STD-2525D.

3.2.5.9.5 Targeting

3.2.5.9.5.1 The software shall allow the user to create and view target lists.

3.2.5.9.5.2 The software shall allow the user to assign a name to target lists.

3.2.5.9.5.3 The software shall require the user to specify the owning unit when creating a target list.

3.2.5.9.5.4 The software shall require the user to specify the status, priority, objective and classification when creating a target list.

3.2.5.9.5.5 The software shall allow the user to associate target lists to an Operation, a mission, an AOR, an AO, an AOI, and to an AI.

3.2.5.9.5.6 The software shall allow the user to add targets to a target list.

3.2.5.9.5.7 The software shall allow the user to add Objects to a target list from the query results, map view, and link analysis view.

3.2.5.9.5.8 The software shall allow the user to set a rank for associated targets on a target list.

3.2.5.9.5.9 The software shall allow the user to prioritize target ranks within a target list.

3.2.5.9.5.10 The software shall allow the user to export target lists to a report template.

3.2.5.9.5.11 The software shall allow the user to send targets and target coordinates from a target list to a map.

3.2.5.9.5.12 The software shall allow the user to send targets from a target list to a link analysis view.

3.2.5.9.5.13 The software shall allow the user to create and edit target card templates.

3.2.5.9.5.14 The software shall allow the user to create target cards from the target card template.

3.2.5.9.5.15 The software shall allow the user to view target and target list properties of a given target card.

3.2.5.9.5.16 The software shall allow the user to create and display target packages for all targets on a target list.

3.2.5.9.5.17 The software shall allow the user to create target packages for single targets on a target list.

3.2.5.9.5.18 Where the selected target is an Object, the target packages shall include the Relationships for the selected target.

3.2.5.9.5.19 The target packages shall include the images, reporting summary, characteristics and identifying attributes for the selected targets.

3.2.5.9.5.20 The software shall allow the user to export target packages to dynamic report types.

3.2.5.10 Capability in Disconnected, Intermittent, and Low-Bandwidth (DIL) Environments

Background

Due to the expeditionary mission of the USMC, the Marines are often operating in degraded or absent network communications environments. The AATS software is intended to operate where the Marines operate – from the fixed sites at the MEF to the Company deployed at a forward operating base. Therefore, the AATS software must be able to support the range of networking challenges encountered, including:

- Intermittent connectivity between the IW and the IS-W
- Intermittent connectivity to other nodes on the MCEN
- Low-bandwidth connectivity between the IW and the IS-W
- Low-bandwidth connectivity to other nodes on the MCEN
- High-latency connections between the IW and the IS-W
- High-latency connections to other nodes on the MCEN

AATS Software Requirements

3.2.5.10.1 The AATS software shall be capable of operating in a DIL network environment for up to 30 days.

3.2.5.10.2 AATS software components installed on the IW shall be capable of operating disconnected from the IS-W for up to 30 days.

3.2.5.10.3 The software shall allow the user to retrieve and store a subset of data locally to allow operations in a disconnected environment.

3.2.5.10.4 The software shall allow the user to edit the subset of data locally.

3.2.5.10.5 The software shall automatically synchronize data upon restoration of network connectivity.

3.2.5.10.6 The option to automatically synchronize data upon restoration shall be user configurable.

3.2.5.10.7 The software shall allow the user to identify changes between the original subset and the edited subset prior to synchronization.

3.2.5.10.8 The software shall allow the user to only synchronize changes from the original dataset.

3.2.5.10.9 The software shall allow the user operating in a DIL network environment to use the data entry capabilities of Section 3.2.5.2.

3.2.5.10.10 The software shall allow the user operating in a DIL network environment to use the map display capabilities of Section 3.2.5.3 utilizing local map imagery.

3.2.5.10.11 The software shall allow the user operating in a DIL network environment to use the data organization capabilities of Section 3.2.5.4.

3.2.5.10.12 The software shall allow the user operating in a DIL network environment to use the search capabilities of Section 3.2.5.5.

3.2.5.10.13 The software shall allow the user operating in a DIL network environment to use the analysis capabilities of Section 3.2.5.6.

3.2.5.10.14 The software shall allow the user operating in a DIL network environment to use the report capabilities of Section 3.2.5.9.3.

3.2.5.10.15 The software shall allow the user operating in a DIL network environment to use the targeting capabilities of section 3.2.5.9.5.

3.2.5.10.16 The software shall allow the user operating in a DIL network environment to use the intelligence journal capabilities of Section 3.2.5.8.

3.2.5.10.17 The software shall provide the capability to deploy ontology updates to nodes operating in a DIL environment.

3.2.5.11 Replication

3.2.5.11.1 The software shall allow data to be replicated to all echelons.

3.2.5.11.2 The software shall allow the user to identify data to be excluded from replication.

3.2.5.11.3 The software shall allow the users to configure replication to exclude files.

3.2.5.11.4 When files are excluded from replication, the file metadata shall still be replicated.

3.2.5.11.5 When the software is configured to exclude files from replication, a remote user shall be capable of retrieving individual files upon request.

3.2.5.11.6 The software shall allow nodes to be publishers, subscribers, or both.

3.2.5.11.7 The software shall be capable of managing conflicts during replication.

3.2.5.11.8 Conflicts shall be stored in a viewable log for comparison.

3.2.5.11.9 Within the conflict log the user shall have the ability to override conflicts and to merge Properties for like Objects.

3.2.5.11.10 The software shall alert the user when replication has been interrupted due to connectivity loss.

3.2.5.11.11 The software shall automatically resume replication upon reestablishing connection.

3.2.5.11.12 The option to automatically resume replication shall be user configurable.

3.2.5.11.13 The software shall allow the user to abort replication.

3.2.5.12 Application Programming Interface (API)

3.2.5.12.1 System Data

Background

In order to integrate the AATS database to external systems, the Government requires an API to allow 3rd-party software access to the AATS database. API access allows 3rd-party software to automate the dissemination of intelligence to external systems, as well as to make intelligence data on external systems available for analysis to the user operating the AATS software.

AATS Software Requirements

3.2.5.12.1.1 The software shall provide an open API to create, read, update, and archive system data.

3.2.5.12.1.2 The API shall restrict access to system data to only authenticated and authorized system users.

3.2.5.12.1.3 The API shall allow 3rd-party software to create, read, update, and archive Object Types in the system ontology.

3.2.5.12.1.4 The API shall allow 3rd-party software to create, read, update, and archive Property Types used by Object Types in the system ontology.

3.2.5.12.1.5 The API shall allow 3rd-party software to create, read, update, and archive Relationship Types in the system ontology.

3.2.5.12.1.6 The API shall allow 3rd-party software to create, read, update, and archive Property Types used by Relationship Types in the system ontology.

3.2.5.12.1.7 The API shall allow 3rd-party software to create, read, update, and archive Objects.

3.2.5.12.1.8 The API shall allow 3rd-party software to set and update Property values.

3.2.5.12.1.9 The API shall allow 3rd-party software to create, update, and archive Relationships.

3.2.5.12.1.10 The API shall allow 3rd-party software to set and update Relationship Property values.

3.2.5.12.1.11 The API shall allow 3rd-party software to perform search queries.

3.2.5.12.2 Analytical Framework

Background

For the development of analytics, the Government requires an efficient framework that allows for analytic plugins to be deployed and executed against the AATS database without the need for developing extensive API calls for data matching a particular query/filter set. In other words, the API must allow analytic plugins to operate on data without the cost of transporting data to and from the database.

AATS Software Requirements

3.2.5.12.2.1 The software shall define an analytic interface and be capable of executing externally defined analytics that conform to the analytic interface.

3.2.5.12.2.2 The software shall allow externally developed analytics to function on incoming data in a streaming manner.

3.2.5.12.2.3 The software shall allow externally developed analytics to function on all resident data at once.

3.2.5.12.2.4 The software shall allow externally developed analytics to utilize the application's filtering capability through the API to set a filter for the data it functions on to specific types (images, text, sound, etc.).

3.2.5.12.2.5 The software shall allow externally developed analytics to store intermediate results in a temporary, non-user visible location.

3.2.5.12.2.6 The software shall allow externally developed analytics to annotate common file types with analytic results (images, text, videos, etc.).

3.2.5.12.2.7 The software shall allow externally developed analytics to alert system users.

3.2.5.12.2.8 The software shall allow externally developed analytics to add data to AATS analytical tools.

3.2.5.12.2.9 The software shall allow externally developed analytics to be initiated by the user on user selected data.

3.2.5.12.3 User Interface Plugins

Background

In order to respond to emerging requirements from the operational user for workflow aids, the Government requires delivery of AATS software with APIs that will be compatible with to allow 3rd-party plugins, which can act as an integral part of the overall AATS software. For example, a user should be able to send a set of selected data from search results (PWS 3.2.5.5) to a 3rd-party plugin that provides a custom, interactive visualization and that visualization can also be sent as an image representation to the production capability (PWS 3.2.5.9).

AATS Software Requirements

3.2.5.12.3.1 The software shall provide the capability for insertion of 3rd-party-developed software plugins that are accessible to the user via the software graphical user interface.

3.2.5.12.3.2 The software shall provide the capability for 3rd-party plugins to receive user-selected data from the interactive elements of the software user interface.

3.2.5.12.3.3 The software shall provide the capability for 3rd-party plugins to send data to the AATS software's Production capabilities described in Section 3.2.5.9.

3.2.5.12.3.4 The software shall provide the capability for 3rd-party plugins to generate and display visualizations of the data.

3.2.5.12.3.5 The software shall provide the capability for 3rd-party plugins to receive selected geospatial data (point coordinate, bounding box, polygon, etc.) from the map display.

3.2.5.12.3.6 The software shall provide the capability for 3rd-party plugins to display data in user-selected layers on the map display.

3.2.5.13 Storage and Backup

3.2.5.13.1 The software shall be capable of storing data in a local repository.

3.2.5.13.2 The software shall allow the user to apply software updates/patches without the loss of data.

3.2.5.13.3 The software shall be capable of creating backups of all mission data.

3.2.5.13.4 The software shall be capable of performing nightly backups.

3.2.5.13.5 The software should be capable of hourly differential backups.

3.2.5.13.6 The software shall be capable of database backup and restore.

3.2.5.13.7 The software should support online backup of the database, allowing continued access to the data during the backup.

3.2.5.14 Cataloging Imagery and Video

Background

Cataloging imagery involves extracting metadata from the imagery (or video) and providing a search capability of the imagery (or video) according to a user-selected metadata field.

Requirements

3.2.5.14.1 The software shall allow the user to catalog imagery.

3.2.5.14.2 The software shall be capable of displaying the following imagery formats:

NITF
JPEG
Bitmap (BMP)
TIFF
Graphic Interchange Format (GIF)
GEOTIFF
JPEG 2000 (JP2)
PNG
WMF
CIB
NSIF

3.2.5.14.3 The software shall allow the user to catalog video.

3.2.5.14.4 The software shall be capable of displaying MPEG-2 and MPEG-4 encoded video files.

3.2.5.15 Collections

3.2.5.15.1 The software shall provide a collections synchronization matrix that displays all the Intelligence Requirements (IRs) within a particular mission.

3.2.5.15.2 The software shall provide a collections synchronization matrix that displays the links between IRs and all associated Objects.

3.2.5.15.3 The software shall provide a collections synchronization matrix that displays the links between IRs and all associated Objects.

3.2.5.15.4 The software shall have the capability to identify a specific attribute value instance within an Object instance when associating to an IR.

3.2.5.15.5 When an Object is selected from the collection synchronization matrix, all associated attribute values shall be displayed first.

3.2.5.16 System Administration

3.2.5.16.1 The software shall support the management of local file stores.

3.2.5.16.2 The software shall support the management of data sources.

3.2.5.16.3 The software shall support the management of services.

3.2.5.16.4 The software shall support the management of local applications.

3.2.5.16.5 IP Addresses shall be configurable by the system administrator.

3.2.5.16.6 Host names shall be configurable by the system administrator.

3.2.5.16.7 Usernames shall be configurable by the system administrator.

3.2.5.16.8 Passwords shall be configurable by the system administrator.

3.2.5.16.9 Database server ids shall be configurable by the system administrator.

3.2.5.16.10 The software shall be able to utilize self-signed and third-party signed security certificates.

3.2.5.16.11 The system administrator account shall be capable of creating passwords for user accounts.

3.2.5.16.12 The system administrator account shall be capable of setting passwords for user accounts.

3.2.5.16.13 The system administrator account shall be capable of assigning profiles to user accounts.

3.2.5.16.14 The system administrator account shall be capable of removing profiles from user accounts.

3.2.5.17 Database Log

3.2.5.17.1 The software shall maintain a complete history of all database updates.

3.2.5.17.2 The software shall record the user name of the user who made the database update.

3.2.5.17.3 The software shall record the DTG when database updates are made.

3.2.5.17.4 The software shall produce a report of all incoming or outgoing reporting and significant events that occurred during a particular timeframe.

3.2.5.17.5 The software shall maintain a complete history and attribution of changes to an individual Object.

3.2.5.17.6 Each time an Object changes, it shall be tagged with a version number.

3.2.5.17.7 The Object history shall be visible to all users authorized to view the current Object.

3.2.5.17.8 The software shall provide the capability to allow approved users to revert to a previous version of an Object.

3.2.5.18 User Permissions

3.2.5.18.1 The software shall allow the system administrator to configure user accounts.

3.2.5.18.2 The software shall have configurable permissions to determine allowable actions on a per user basis.

3.2.5.18.3 The software shall only display data permitted by the user's role.

3.2.5.19 Help Function

The software shall provide a context-sensitive help link to the user.

3.2.5.20 Computer Communications Requirements

3.2.5.20.1 The software shall support Internet Protocol Version 4 (IPv4).

3.2.5.20.2 The software shall support Internet Protocol Version 6 (IPv6).

3.2.6 Licensing

3.2.6.1 (CLIN 0001 and CLIN 0011) The IAS FoS Tier I and II includes 152 independent and geographically dispersed server systems, each of which supports one or more of the 2574 Tier III Intelligence Workstations. AATS software user licenses for the IW shall provide all of the required software licenses for the server and client software components that comprise the AATS software, not including operating system licenses.

(CLIN 0001) Within 90 days of delivery order 0001 issuance, the contractor shall deliver to SPAWARSYSCEN Atlantic software user licenses (nine users) for the AATS software to be used by IAS personnel for the engineering and logistics activities required to incorporate the software package onto the IAS software baseline. The contractor shall also provide software sustainment, software updates, and security updates for the AATS software.

(CLIN 0001) Additionally, the contractor shall deliver to SPAWARSYSCEN Atlantic software user licenses (2574 users) for follow-on fielding of AATS software to Marine Corps operating forces. The effective date for software user licenses issued under CLIN 0001 shall be the date of delivery of the software user licenses. . The contractor shall also provide software sustainment, software updates, and security updates for the AATS software.

(CLIN 0011) The contractor shall deliver to SPAWARSYSCEN Atlantic additional software user licenses/user capacity as purchased under CLIN 0011 to support and expand the IAS FoS Authorized Acquisition Objective (AAO) in increments of 100 users. The effective date for additional software user licenses shall continue from the purchase date through the end of the contract performance period. The contractor shall provide software sustainment, software updates, and security updates for the additional user license/user capacity through the end of the contract performance period.

3.2.6.2 The contractor shall provide a local system licensing mechanism that can be utilized pre-deployment

and must operate on SIPRNET and in a DIL network environment. The licensing mechanism must not be dependent upon resources beyond those available on SIPRNET and in a DIL network environment.

3.3 TECHNICAL DATA

3.3.1 Data Rights

3.3.1.1 To the maximum extent practicable, the Government will require delivery of Technical Data (TD) and Computer Software (CS) under the AATS contract with license rights and data rights as necessary to support the sustainment of the AATS within the Intelligence Analysis System (IAS) program (e.g., open systems architecture and future competitions), both within and outside the Government.

3.3.1.2 The Government will have unlimited rights in non-commercial TD/CS that is funded exclusively at Government expense and rights no more restrictive than Government Purpose Rights (GPR) in all non-commercial TD/CS that is developed partially at Government expense.

3.3.1.3 Each offeror shall describe in its proposal all commercial computer software and technical data that will be used in the performance of the contract, and forward copies of all applicable licenses. The Government will review such licenses to ensure the licenses are consistent with federal procurement law. Each offeror shall explicitly state whether each commercial computer software component utilized in their proposed AATS software product will be needed by the Government to sustain the AATS system at the end of the contract (see solicitation provisions 252.227-7017, 252.227-7028, and 5252.227-9216, evaluation subfactor A4 (Interoperability and Open Systems Architecture), and solicitation Attachment 15 (Software License Disclosure)).

3.3.1.4 If the projected AATS software deliverables include non-commercial development that is layered over CI or NDI components, the offeror shall fully describe all interfaces between the non-commercial and commercial portions of the AATS software. Proposals shall also address the extent to which the Contractor proposes to deliver the interfaces with at least Government Purpose Rights (GPR), or its commercial equivalent, i.e., the rights to distribute the interfaces outside of Government to third parties, for purposes where Government is a party (including reprocurements), but under conditions which prevent the third party from further distribution.

3.3.1.5 Each offeror shall discuss its rationale for proposing any TD/CS with rights more restrictive than GPR and how such restrictive rights will not harm IAS program goals. An offeror's proposal that imposes license restrictions more restrictive than GPR will be scrutinized to ensure that such restrictions will not negatively impact the IAS program, in terms of the Government's ability to sustain AATS at its discretion, either by itself or via a third party (see solicitation provisions 252.227-7017, 252.227-7028, and 5252.227-9216, evaluation subfactor A4 (Interoperability and Open Systems Architecture), and solicitation Attachment 15 (Software License Disclosure)).

3.3.1.6 The Government shall be able to integrate, with any commercial portion of the solution, existing or future Government-developed features using Government-developed interfaces without requiring pre-approval by the offeror.

3.3.1.7 The Government shall have unlimited data rights to all data input into, stored in, and output from the AATS software package. The Government requires that any data that passes through, is processed by, or otherwise interacts with the commercial portion of the AATS software will be wholly owned by the Government before, during, and after such interaction, and that such data will neither be encumbered by any proprietary information of the offeror or be transformed or otherwise modified into a format that renders it unsuitable for the Government's purposes as set forth in the solicitation.

3.3.2 Technical Data Documentation

The contractor shall provide technical data documentation that is sufficient to allow Government and support contractor IAS personnel in the engineering and logistics activities to incorporate the software package onto the IAS software baseline. Technical documentation shall be in electronic (searchable and digital) format, and in paper

format as requested. Technical data that supports the following AATS technical documentation will be necessary (CDRL A001)(CDRL A002)(CDRL A003)(CDRL A004)(CDRL A018).

Engineering (CLIN 0002)

(a) Software Version Description
(b) Software Architecture Diagrams
(c) Software Installation Instructions
(d) Software Build List
(e) Software Troubleshooting Guide
(f) Database Design
(f) Application Programming Interface Documentation
(g) Software Development Guide
(h) All open Software Trouble Reports filed against the software package version delivered
(i) Software Development Plan

Logistics (CLIN 0002)

(a) Quick Reference Guide (General)
(b) Installation Guide/Manual
(c) Instruction Manual
(d) System Administrator Manual (SAM)
(e) System User Manual (SUM)
(f) License Activation Instructions

Training (CLIN 0003)

(a) Training Materials

3.4. SYSTEMS ENGINEERING SUPPORT SERVICES

3.4.1 Implementation Planning (CLIN 0004)

3.4.1.1 The contractor shall participate in implementation planning meetings with Program Management Office (PMO) and other Government personnel. The contractor shall develop an approach for implementation of the AATS software on the IAS software baselines that meets specified price, schedule, and performance constraints of the IAS program.

3.4.1.2 The contractor shall prepare reports, plans, summaries, and/or briefings (CDRL A002) that describe the implementation plan. Unless specified otherwise in each TO, the Contractor's format is acceptable.

3.4.2 Software Installation (CLIN 0004)

The contractor shall support SPAWARSYSCEN Atlantic IAS personnel in the installation of AATS software components on the IW and IS-W.

3.4.2.1 The contractor shall assist SPAWARSYSCEN Atlantic IAS personnel with resolution of AATS software installation failures through identification of acceptable workarounds and/or issuance of AATS software patches. Resolutions will be considered acceptable when the AATS software installs correctly without impact to other software on the same platform.

3.4.2.2 The contractor shall assist SPAWARSYSCEN Atlantic IAS personnel with resolution of AATS-related software trouble reports (STRs) through identification of acceptable workarounds and/or issuance of AATS

software patches. STR resolutions will be verified by the IAS test team, and STRs will be closed by determination of the IAS Change Review Board (CRB).

3.4.2.3 The contractor shall assist SPAWARSYSCEN Atlantic IAS personnel with acceptable resolution of discovered vulnerabilities that are associated with the AATS software application. Resolution will be considered acceptable by determination of IAS Information Assurance (IA) personnel.

3.4.2.4 The contractor shall prepare a report (CDRL A002) documenting all implemented resolutions for AATS software installation failures and AATS software trouble reports. The report shall document the problem, the root cause, and the resolution. If the resolution is a workaround, the report shall document the workaround steps in detail. Unless specified otherwise in each TO, the Contractor's format is acceptable.

3.4.2.5 The contractor shall prepare a report (CDRL A002) documenting all implemented resolutions for vulnerabilities that are associated with the AATS software application. The report shall document the problem, the root cause, and the resolution. Unless specified otherwise in each TO, the Contractor's format is acceptable.

3.4.3 Software Engineering (CLIN 0009)

Background

The Government expects to receive feedback from the end-users from the fielding and deployment of the AATS software, and the subsequent day-to-day use of the AATS software. In addition, evolving threats and interests will give rise to demand for additional capabilities to meet these challenges. The Government plans to track these requests for modifications to the AATS software, and develop additional functional requirements within the scope of the service-level operational requirements. These requirements will become the basis of product improvement efforts for the AATS software.

Requirements

The contractor shall provide software engineering, information assurance, and scientific disciplines to support the implementation of emerging functional requirements for the AATS software. This support includes planning, designing, programming, testing, integrating, and delivering algorithms and software (source code and executables). CI or NDI solutions and product modifications (e.g., software tools, licensing, and associated hardware) which are incidental to the overall support service efforts are considered within the scope of this requirement. At the task order level, specific technical approaches and process management assessments to software development shall be required.

The contractor shall prepare a report (CDRL A002) that documents the design, implementation, installation, configuration, troubleshooting, and usage of any software developed in support of product improvement efforts directed by the Government under each TO. Unless specified otherwise in each TO, the Contractor's format is acceptable.

The contractor shall provide the Government (and/or Government support contractors) electronic access to its integrated digital (or development) environment (IDE) and the ability to download draft artifacts (actual delivery of software artifacts will be in accordance with CDRL A002) throughout the term of the contract. The Government reserves the right to witness all Contractor efforts to accomplish the PWS requirements and maintains the right to comment on processes.

The contractor shall provide the Government (and/or Government support contractors) real-time access to the contractor's (and any associated subcontractor's) software development environment, providing the Government with continuous online access to and the ability to download work products under development commencing at the time of delivery order award.

The contractor shall develop software upgrades and software capabilities that ensure that:

Data will be posted to shared spaces for users to access and download except when limited by security, policy, or regulations;

Data shall provide for interoperability with many-to-many exchanges of data, and verified trust and integrity of users and applications; and

Data shall be transmitted through well and openly defined interfaces.

The contractor shall ensure that its projects, at the architectural and operational level, continue to promote the use of an open architecture as well as adoption of other standards and requirements, tailored to meet its specific Service and Joint requirements.

3.4.3.1 Modular Open Systems Approach (MOSA)

As directed at the task order level, the contractor shall describe its rationale for the modularization choices made to generate the design. The contractor's design approach shall produce a system that consists of hierarchical collections of software configuration items (components). These components shall be of a size that supports competitive acquisition as well as reuse. The contractor's design approach shall emphasize the selection of components that are available commercially or within the DoD, to avoid the need to redevelop products that already exist and that can be reused. The contractor's rationale shall explicitly address any tradeoffs performed, particularly those that compromise the modular and open nature of the system.

3.4.3.2 Life Cycle Sustainability

The contractor shall consider use of commercial item/NDI and open standards to enhance the system's life cycle sustainability by implementing performance-based logistics (PBL) arrangements to sustain the components through their life cycle.

3.4.3.3 Interface Design and Management

As directed at the task order level, the contractor shall:

Clearly define, identify, and describe all component and system interfaces;

Define and document all subsystem and configuration item (CI) level interfaces to provide full functional, logical, and physical specifications;

Identify the interface and data exchange standards between the component, module or system and the interconnectivity or underlying information exchange medium;

Use the identified interfaces to support an overall information assurance strategy that implements Information Assurance (IA) Processes in accordance with DoD Instruction 8500.2 (dated February 6, 2003) and;

If applicable, select external interfaces from existing open or Government standards with an emphasis on enterprise-level interoperability. The contractor shall describe how its selection of interfaces will maximize the ability of the system to easily accommodate technology and facilitate the insertion of alternative or reusable modular system elements on either side of the interface.

3.4.3.4 Reuse of Pre-existing or Common Items

As directed at the task order level, the contractor shall reuse pre-existing or common items unless a determination is made to not reuse. Exceptions to reuse of pre-existing items must be accompanied by justification, such as price (both of adoption and life cycle support), schedule, functional and non-functional performance, etc. The general objective of these efforts shall be the development of a common system and/or common elements or components

which meet the performance requirements of the various DoD or Service platform missions, where commonality offers the greatest technical and cost benefits.

3.4.3.5 Open Business Practices

As directed at the task order level, the contractor shall demonstrate that the modularity of the system design promotes the identification of multiple sources of supply and/or repair, and supports flexible business strategies that enhance subcontractor competition. The contractor shall conduct a market survey to identify candidate commercial items, proprietary, open source software (OSS), and other reusable NDIs capable of achieving the performance requirements of solutions that it proposes to custom build. The survey results shall be provided to support each major review. Commercial items and other reusable NDI selection criteria shall address the following factors, at a minimum: reliability consistent with the environment described in this PWS; maintainability; subsystem performance trade-offs; open system architecture break out compatibility; cost; manufacturer's quality assurance provisions; market acceptability; obsolescence; adequacy of available technical and intellectual property data and re-procurement data rights on the product; and merits of the software supported by the product. Decisions leading to the selection of specific commercial items, NDI, proprietary or OSS products should be supported by appropriate analysis (e.g., with test results, architectural suitability, "best value" assessments, etc.).

3.4.3.6 Software Development Plan (SDP)

The contractor shall define a software development approach appropriate for the computer software effort to be performed under each task order. The contractor shall follow this software development approach for all computer software to be developed or maintained under this effort. At a minimum, the SDP (CDRL A018) shall meet the following criteria:

3.4.3.6.1 When required at task order level, the SDP shall be initially delivered to the Government no later than (NLT) 30 days after task order award and NLT commencement of software activity. No specific format is required; the document is content driven. Subject to review, the SDP shall be placed under configuration control after it has been approved by the Government. The document shall be resubmitted for review and Government approval when periodic updates are performed subsequent to process improvement reviews.

3.4.3.6.2 The SDP shall document all System Life Cycle Processes applicable to the system to be acquired, as defined by IEEE Std. 12207 – 2008 as appropriate.

3.4.3.6.3 The SDP shall define the contractor's proposed life cycle model and the processes used as a part of that model. In this context, the term "System Life Cycle Processes" is as defined in IEEE Std. 12207 - 2008. The SDP shall describe the System Life Cycle Processes applicable to the software to be acquired based on the work content of the Task Order.

In accordance with the framework defined in IEEE Std. 12207 - 2008, the SDP shall define the processes, the activities to be performed as a part of the processes, the tasks which support the activities, and the techniques and tools to be used to perform the tasks.

3.4.3.6.4 The SDP shall contain the information defined by IEEE/EIA Std. 12207.1, section 5.2 (generic content) and the Plans or Procedures in Table 1 of IEEE/EIA Std. 12207.1. The content of the SDP shall be tailored to contain only the information and sections that are applicable to the tasks defined in the task order. If any information item is not relevant to either the system or to the proposed process, that item is not required.

3.4.3.6.5 The SDP shall adhere to the characteristics defined in section 4.2.3 of IEEE/EIA Std. 12207.1, as appropriate. In all cases, the level of detail shall be sufficient to define all software development processes, activities, and tasks to be conducted which will allow the use of the SDP as the full guidance for the developers. In accordance with section 6.5.3b of IEEE/EIA Std. 12207.1, information provided must include, as minimum, specific standards, methods, tools, actions, reuse strategies, and responsibilities associated with development and qualification including safety and security.

3.4.4 Ontology Installation (CLIN 0004)

3.4.4.1 The contractor shall support SPAWARSYSCEN Atlantic IAS personnel with the installation of the Government-provided ontology into the AATS software package.

3.4.4.2 The contractor shall support SPAWARSYSCEN Atlantic IAS personnel with resolution of software trouble reports and change requests related to the installed ontology. Resolutions will be considered acceptable by determination of the IAS CRB.

3.4.4.3 The contractor shall prepare a report (CDRL A002) documenting all implemented resolutions for software trouble reports and change requests related to the installed ontology. The report shall document the problem, the root cause, and the resolution. If the resolution is a workaround, the report shall document the workaround steps in detail. Unless specified otherwise in each TO, the Contractor's format is acceptable.

3.4.5 Data Integration (CLIN 0004)

3.4.5.1 The contractor shall support SPAWARSYSCEN Atlantic IAS personnel with the integration of data sources to the AATS software package.

3.4.5.2 The contractor shall prepare a design document (CDRL A002) that documents the interface between the data source and the AATS software package, the data management strategy, the mapping of information from the data source to the AATS ontology, the configuration parameters, and all other technical data required for the IAS program to maintain the data integration. Unless specified otherwise in each TO, the Contractor's format is acceptable.

3.4.5.3 The contractor shall prepare a report (CDRL A002) that documents the installation, configuration, troubleshooting, and usage of the data integration. Unless specified otherwise in each TO, the Contractor's format is acceptable.

3.4.6 Cybersecurity/Information Assurance (CLIN 0004)

Cybersecurity (also known as Information Assurance (IA)) includes tasks which the contractor shall protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

3.4.6.1 Cybersecurity Personnel

(a) In accordance with DFAR clause 252.239-7001, DoDD 8570.01 and SECNAV M-5239.2, contractor personnel performing cybersecurity functions shall meet all cybersecurity training, certification, and tracking requirements as cited in DoD 8570.01-M prior to accessing DoD information systems.

(b) The contractor shall be responsible for tracking and reporting cybersecurity personnel, also known as Cyber Security Workforce (CSWF). See PWS Para 5.2.1.4 for CSWF Report (CDRL A009) requirements. Although the standard frequency of reporting is monthly, the task order can require additional updates at any time.

3.4.6.2 Design Changes
The contractor shall ensure any equipment/system installed or integrated into Navy platform will meet the cybersecurity requirements as specified under DoDI 8500.01.

3.4.6.3 IA Support Requirements

3.4.6.3.1 The contractor shall provide qualified (per DoD 8570.01) Information Assurance Manager (IAM) Level II personnel to support IAS IA personnel in the preparation of system documentation required for an Authority to Operate (ATO) determination from the Designated Approving Authority (DAA).

3.4.6.3.2 The contractor shall review AATS-related findings listed in Government-provided Assured Compliance Assessment Solution (ACAS) scan reports, and shall prepare a response to the finding. Responses will be considered acceptable by determination of IAS IA personnel.

3.4.6.3.3 Source Code Analysis

The contractor shall assist IAS software assurance personnel in the instrumentation of automated source code analysis tools for review of source code developed under this contract.

The contractor shall review findings from automated source code analysis, and shall prepare and implement a response to the finding. Responses will be considered acceptable by determination of IAS IA personnel.

3.4.6.3.4 Security Technical Implementation

3.4.6.3.4.1 Technical Planning

The contractor shall participate in information assurance planning meetings with Program Management Office (PMO) and SPAWARSYSCEN Atlantic IAS personnel. The contractor shall identify all AATS software components in sufficient detail to allow IAS personnel to determine the applicable DISA guidance documents for each AATS software component.

The contractor shall prepare a report (CDRL A002) that documents the AATS software components and the applicable DISA guidance document for each AATS software component. Unless specified otherwise in each TO, the Contractor's format is acceptable.

3.4.6.3.4.2 Technical Execution

The contractor shall review each IAS identified security requirement from the DISA guidance documents review identified in Paragraph 3.4.6.3.4.1 (Technical Planning) and develop a response to the requirement. Response will be considered acceptable by determination of IAS Information Assurance (IA) personnel.

If the security requirement is not applicable to the AATS software component, then the response shall provide detailed justification to support a "Not Applicable" determination.

If the security requirement is applicable to the AATS software component, then the response shall provide the steps required to configure the software to meet the requirement, and the steps required to verify the configuration.

The contractor shall provide software updates or patches to meet all applicable security requirements that cannot be met through post-installation configuration of the software component.

The contractor shall prepare a report (CDRL A002) that documents all responses to security requirements for each AATS software component. Unless specified otherwise in each TO, the Contractor's format is acceptable.

3.4.7 Testing (CLIN 0004)

3.4.7.1 The contractor shall provide expertise with establishing, implementing, and conducting software tests, including Software Item (SI) integration testing and Software Unit (SU) testing.

3.4.7.2 The contractor shall provide support to IAS test personnel in the development and execution of tests of AATS software in accordance with software testing practices outlined in IEEE/EIA 12207. Support services include:

3.4.7.3 Test Documents

3.4.7.3.1 The contractor shall develop (CDRL A002) Test Cases and Test Procedures to support development testing (DT) and operational testing (OT) of AATS software components on the IAS software baseline.

Test Cases and Test Procedures shall be in Microsoft Excel format.

Content of Test Cases and Test Procedures shall be in accordance with IEEE Std 829-2008.

3.4.7.3.2 The contractor shall provide troubleshooting and resolution of test incidents and other technical support issues encountered during test events.

The contractor shall document all test incidents related to AATS software. Unless specified otherwise in each TO, the Contractor's format is acceptable.

3.4.7.4 Automated Test Support

The contractor shall support IAS test personnel in the development of automated test scripts for automated user interface-driven testing of the AATS software.

3.4.7.5 Performance Testing

3.4.7.5.1 Planning

The contractor shall participate in planning meetings with PMO and SPAWARSYSCEN Atlantic personnel to identify performance test objectives and resource, technical, and schedule requirements.

The contractor shall prepare a Performance Test Plan (CDRL A002) in Microsoft Word format.

The contractor shall prepare Performance Test Cases (CDRL A002) in Microsoft Excel format.

Content of Performance Test Cases shall be in accordance with IEEE Std 829-2008.

3.4.7.5.2 Execution

The contractor shall execute a performance test of the AATS software components on the IAS software baseline in accordance with the Performance Test Plan.

The contractor shall prepare a Performance Test Report (CDRL A002) in Microsoft Word format that documents the test architecture, test configuration, and issues encountered during the test.

The contractor shall provide the Performance Test Results (CDRL A002) in Microsoft Excel format.

3.5 FIELDING AND TRAINING SERVICES

3.5.1 Training Package

3.5.1.1 Initial Training (CLIN 0003): The contractor shall develop Systems Approach to Training (SAT) compliant training material and lesson plans to provide operator training on new system software as delineated in the Job Task Analysis (JTA) (CDRL A004). All documents produced under this contract are the property of the United

States Government. The United States Government reserves the right to modify, reproduce, distribute, perform, display, release, or disclose for any purpose documents under this contract.

3.5.1.2 Updates (CLINs 0005, 0006, 0007, 0008): When software package version upgrades are provided, the contractor shall update SAT compliant training material and lesson plans and provide operator training on the updated system software as delineated in the JTA (CDRL A004).

3.5.1.3 Product Improvement Periods (CLIN 0009): During product improvement periods the contractor shall update SAT compliant training material and lesson plans and provide operator training on the updated system software as delineated in the JTA (CDRL A004).

3.5.2 New Equipment Training and Fielding Support (CLIN 0004)

3.5.2.1 Background

New Equipment Training (NET) is provided to the operational forces at I, II, and III MEF, Marine Forces Reserve (MFR), and Supporting Establishment. NET consists of refresher training, tailored unit training, "just in time" training, and/or exercise support training. The IAS Training Team is responsible for the development and maintenance of training materials as related to the currently fielded IAS software baseline. The IAS Training Team leaves the unit with hard and/or soft copies of the training material.

3.5.2.2 The contractor shall support and provide AATS software expertise while conducting NET per the Fielding Plan.

3.5.2.3 The contractor shall conduct NET on the AATS software per the Fielding Plan.

3.5.2.4 The contractor, in accordance with the Project Office-provided fielding schedule, shall support the IAS Training Team during NET to the operational forces at I, II, and III MEF, MFR, and Supporting Establishment, at the following locations:

Marine Corps Intelligence Activity, Quantico, VA
Marine Corps Base, Camp Lejeune, NC (II MEF and MARSOC)
Marine Corps Base, Cherry Point, NC (II MAW)
Marine Corps Base, Camp Pendleton, CA (I MEF, MARSOC West)
Marine Corps Base, Miramar, CA (III MAW)
Marine Corps Base, Okinawa, Japan (III MEF)
Marine Corps Base, Iwakuni, Japan (I MAW)
Marine Corps Intelligence School, Dam Neck, VA
Marine Corps Base, Oahu, HI (3d Marines)

3.5.2.5 The contractor shall provide a trip report (CDRL A005) at the end of each NET that includes a detailed class roster and student course and instructor critique sheets.

3.5.3 Key Personnel Training (CLIN 0004)

The contractor shall provide key personnel training on the AATS software to SPAWAR Systems Center, MARCORSYSCOM, and contractor support personnel.

3.5.4 Help Desk/Customer Support (CLIN 0001, 0005, 0006, 0007, 0008, 0009)

The Contractor shall provide AATS expertise consultant services to the IAS FoS Help Desk as necessary for the Help Desk to respond to customer AATS issues.

3.5.5 Product Demonstrations (CLIN 0004)

The contractor shall be available to attend and/or facilitate product demonstrations at the request of the User Community and as directed by the Contracting Officer's Representative (COR).

3.5.6 Product Improvement Training (CLIN 0009)

The contractor shall provide AATS technical expertise in support of new equipment training "Delta NET" to units being equipped with Technical Refresh systems.

4.0 INFORMATION TECHNOLOGY (IT) SERVICES REQUIREMENTS

4.1 INFORMATION TECHNOLOGY (IT) GENERAL REQUIREMENTS

When applicable, the contractor shall be responsible for the following:

4.1.1 Ensure that no production systems are operational on any Research Development Test and Evaluation (RDT&E) network.

4.1.2 Follow DoDI 8510.01 of 12 Mar 2014 when deploying, integrating, and implementing IT capabilities.

4.1.3 Migrate all Navy Ashore production systems to the NMCI environment where available.

4.1.4 Work with Government personnel to ensure compliance with all current Navy IT & cybersecurity policies, including those pertaining to Cyber Asset Reduction and Security (CARS).

4.1.5 Follow SECNAVINST 5239.3B of 17 June 2009 & DoDI 8510.01 of 12 Mar 2014 prior to integration and implementation of IT solutions or systems.

4.1.6 Register any contractor-owned or contractor-maintained IT systems utilized on contract in the Department of Defense IT Portfolio Registry (DITPR)-DON.

4.2 ACQUISITION OF COMMERCIAL SOFTWARE PRODUCTS, HARDWARE, AND RELATED SERVICES

Contractors recommending or purchasing commercial software products, hardware, and related services supporting Navy programs and projects shall ensure they recommend or procure items from approved sources in accordance with the latest DoN and DoD policies.

4.2.1 DoN Enterprise Licensing Agreement/DoD Enterprise Software Initiative Program
Pursuant to DoN Memorandum – Mandatory use of DoN Enterprise Licensing Agreement (ELA) dtd 22 Feb 12, contractors that are authorized to use Government supply sources per FAR 51.101 shall verify if the product is attainable through DoN ELAs and if so, procure that item in accordance with appropriate ELA procedures. If an item is not attainable through the DoN ELA program, contractors shall then utilize DoD Enterprise Software Initiative (ESI) program (see DFARS 208.74) and Government-wide SmartBuy program (see DoD memo dtd 22 Dec 05). The contractor shall ensure any items purchased outside these programs have the required approved waivers as applicable to the program. Software requirements will be specified at the TO/contract level.

4.2.2 DoN Application and Database Management System (DADMS)
The contractor shall ensure that no Functional Area Manager (FAM) disapproved applications are integrated, installed or operational on Navy networks. The contractor shall ensure that all databases that use database management systems (DBMS) designed, implemented, and/or hosted on servers and/or mainframes supporting Navy applications and systems be registered in DoN Application and Database Management System (DADMS) and are

FAM approved. All integrated, installed, or operational applications hosted on Navy networks must also be registered in DADMS and approved by the FAM. No operational systems or applications will be integrated, installed, or operational on the RDT&E network.

5.0 CONTRACT ADMINISTRATION

Contract Administration is required for all contracts; it provides the Government a means for contract management and monitoring. Regardless of the level of support, the ultimate objective of the contractor is ensuring the Government's requirements are met, delivered on schedule, and performed within budget.

5.1 CONTRACT LIAISON

The contractor shall assign a technical single point of contact, also known as the Program Manager (PM) who shall work closely with the Government Contracting Officer and Contracting Officer's Representative (COR), as applicable. Note: As this is an Indefinite Delivery/Indefinite Quantity (IDIQ) contracts, CORs will be assigned at the task or delivery order level. The contractor PM, located in the contractor's facility, shall ultimately be responsible for ensuring that the contractor's performance meets all Government contracting requirements within price and schedule. PM shall have the requisite authority for full control over all company resources necessary for contract performance. The PM shall have authority to approve task order proposals or modifications in emergent situations. The PM shall ultimately be responsible for the following: personnel management; management of Government material and assets; and personnel and facility security. In support of open communication, the contractor shall initiate, unless otherwise directed at the task order level, periodic meetings with the COR.

5.2 CONTRACT MONITORING AND MAINTENANCE

The contractor shall have processes established in order to provide all necessary resources and documentation during various times throughout the day in order to facilitate a timely task order (TO) award or modification. Prior to task order award, the contractor shall be responsible for providing any required support documentation in a timely manner so as to not disrupt the TO award process. To address urgent requirements, the contractor shall have processes established during business and non-business hours/days in order to provide all necessary documentation and resources to facilitate a timely TO award or modification. *NOTE: Directly billing to a TO prior to TO award is prohibited.*

5.2.1 Contract Administration Documentation

Various types of contract administration documents are required throughout the life of the contract. At a minimum, the contractor shall provide the following documentation, unless otherwise specified:

5.2.1.1 Contract Status Report (CSR)

The contractor shall develop a Contract Status Report (CDRL A006) and submit it monthly at least 30 days after contract award on the 10th of each month. Only one report is submitted per contract. The prime shall be responsible for collecting, integrating, and reporting all subcontractor reports. The contractor shall report on various contract functions: performance, schedule, financial, business relations, and staffing plan/key personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. This CDRL includes a Staffing Plan (CDRL A006, Attachment 1) necessary for additional data collection as applicable.

5.2.1.2 Task Order Status Report (TOSR)

The contractor shall develop a Task Order Status Reports (CDRL A007) and submit it monthly, weekly, and/or as cited in the requirements of each task order. The prime shall be responsible for collecting, integrating, and reporting all subcontractor reports. The TOSR include the following variations of reports:

(a) Monthly TOSR – the contractor shall develop and submit a TO status report monthly at least 30 days after TO award on the 10th of each month for those months the TO is active. The contractor shall report on various TO functions: performance, schedule, financial, business relations, and staffing plan/key personnel; see applicable

DD Form 1423 for additional reporting details and distribution instructions. This CDRL includes a Staffing Plan (CDRL A006, Attachment 1) necessary for additional data collection as applicable.

(b) Weekly TOSR – the contractor shall develop and submit a weekly TO Status Report which is e-mailed to the COR no later than close of business (COB) every Friday. The first report is required on the first Friday following the first full week after the TO award date. The contractor shall ensure the initial report includes a projected Plan Of Action and Milestones (POA&M). In lieu of a formal weekly report, larger, more complex TOs requires an updated Earned Value Management report. At a minimum unless otherwise noted, the contractor shall include in the weekly report the following items and data:

1. Percentage of work completed
2. Percentage of funds expended per ship/sub/shore command and system
3. Updates to the POA&M and narratives to explain any variances
4. If applicable, notification when obligated funds have exceeded 75% of the amount authorized

(c) Data Calls – the contractor shall develop and submit a data call report which is e-mailed to the COR within six working hours of the request, unless otherwise specified by TO. The contractor shall ensure all information provided is the most current. Funding data will reflect real-time balances. Report will account for all planned, obligated, and expended charges and hours. At a minimum unless otherwise noted, the contractor shall include in the data call the following items and data:

1. Percentage of work completed
2. Percentage of funds expended
3. Updates to the POA&M and narratives to explain any variances
4. List of personnel (by location, security clearance, quantity)
5. Most current CAP listing

5.2.1.3 Contract Closeout Report

The contractor shall develop a task order (TO) closeout report (CDRL A008) and submit it no later than 15 days before the TO completion date. The Prime shall be responsible for collecting, integrating, and reporting all subcontracting information. See applicable DD Form 1423 for additional reporting details and distribution instructions.

5.2.1.4 Cybersecurity Workforce (CSWF) Report

DoD 8570.01-M and DFAR's PGI 239.7102-3 have promulgated that contractor personnel shall have documented current cybersecurity certification status within their contract. The contractor shall develop, maintain, and submit a CSWF Report (CDRL A009) monthly or as applicable at the task order level (Note: If initiated at the TO level, report not necessary at contract level). IAW clause DFARS 252.239-7001, if cybersecurity support is provided, the contractor shall provide a Cybersecurity Workforce (CSWF) list that identifies those individuals who are IA trained and certified. Utilizing the format provided in CSWF CDRL Attachment 1, the prime contractor shall be responsible for collecting, integrating, and reporting all subcontractor personnel. See applicable DD Form 1423 for additional reporting details and distribution instructions. Contractor shall verify with the COR or other Government representative the proper labor category cybersecurity designation and certification requirements.

5.2.1.5 RESERVED

5.2.1.6 WAWF Invoicing Notification and Support Documentation

Pursuant to DFARS clause 252.232-7003 and 252.232-7006, the contractor shall submit payment requests and receiving reports using DoD Invoicing, Receipt, Acceptance, and Property Transfer (iRAPT) application (part of the Wide Area Work Flow (WAWF) e-Business Suite) which is a secure Government web-based system for electronic invoicing, receipt, and acceptance. In accordance with clause 252.232-7006, the contractor shall provide e-mail notification to the COR when payment requests are submitted to the iRAPT/WAWF. As requested, the contractor shall directly provide a soft copy of the invoice and any supporting invoice documentation (CDRL A011) directly to the COR within 24 hours of request to assist in validating the invoiced amount against the products/services provided during the billing cycle.

5.2.1.7 RESERVED

5.2.1.8 RESERVED

5.3 EARNED VALUE MANAGEMENT (EVM)

In accordance with DoD policy, this contract does not require Earned Value Management (EVM) implementation due to the contract type of this contract being Firm-Fixed-Price (FFP).

6.0 QUALITY

6.1 QUALITY SYSTEM

Upon contract award, the prime contractor shall have and maintain a quality assurance process that meets contract requirements and program objectives while ensuring customer satisfaction and defect-free products/process. The contractor shall have a sufficiently documented quality system which contains procedures, planning, and all other documentation and data necessary to provide an efficient and effective quality system based on a contractor's internal auditing system. Thirty (30) days after contract award, the contractor shall provide to the Government a copy of its Quality Assurance Plan (QAP) and any other quality related documents (CDRL A014) as applicable to the TO. The contractor shall make the quality system available to the Government for review at both a program and worksite services level during predetermined visits. Existing quality documents that meet the requirements of this contract may continue to be used. If any quality documentation is disapproved or requires revisions, the contractor shall correct the problem(s) and submit revised documentation NLT 2 weeks after initial disapproval notification. The contractor shall also require all subcontractors to possess a quality assurance and control program commensurate with the services and supplies to be provided as determined by the prime's internal audit system. The Government reserves the right to disapprove the contractor's and/or subcontractor's quality system or portions thereof when the quality system(s) fails to meet contractual requirements at either the program or worksite services level. The Government reserves the right to participate in the process improvement elements of the contractor's quality assurance plan and development of quality related documents as needed. At a minimum, the contractor shall ensure their quality system meets the following key criteria:

- Establish documented, capable, and repeatable processes
- Track issues and associated changes needed
- Monitor and control critical product and process variations
- Establish mechanisms for feedback of field product performance
- Implement and effective root-cause analysis and corrective action system
- Establish methods and procedures for continuous process improvement

6.2 QUALITY MANAGEMENT PROCESS COMPLIANCE

6.2.1 General

The contractor shall have processes in place that coincide with the Government's quality management processes. The contractor shall use best industry practices including, when applicable, ISO/IEC 15288 for System life cycle processes and ISO/IEC 12207 for Software life cycle processes. As applicable, the contractor shall also support and/or participate in event-driven milestones and reviews as stated in the Defense Acquisition University's (DAU's) DoD Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System Chart which is incorporates multiple DoD directives and instructions – specifically DoDD 5000.01 and DoDI 5000.02. The contractor shall provide technical program and project management support that will mitigate the risks to successful program execution including employment of Lean Six Sigma methodologies in compliance with SPAWARSYSCEN Atlantic requirements and with the SPAWARSYSCEN Engineering Process Office (EPO) Capability Maturity Model Integration (CMMI) program. As part of a team, the contractor shall support projects at SPAWARSYSCEN Atlantic that are currently, or in the process of, being assessed under the SPAWARSYSCEN EPO CMMI program. The contractor shall be required to utilize the processes and procedures already established

for the project and the SPAWARSYSCEN EPO CMMI program and deliver products that are compliant with the aforementioned processes and procedures. Although having a formal CMMI appraisal is desired, it is not required.

6.3 QUALITY ASSURANCE

The contractor shall perform all quality assurance process audits necessary in the performance of the various tasks as assigned and identified by the respective WBS, POA&M, or quality system, and the contractor shall deliver related quality plan/procedural documents upon request. The Government reserves the right to perform any additional audits deemed necessary to assure that the contractor processes and related services, documents, and material meet the prescribed requirements and to reject any or all processes or related services, documents, and material in a category when noncompliance is established.

6.4 QUALITY CONTROL

The contractor shall perform all quality control inspections necessary in the performance of the various tasks as assigned and identified by the respective WBS, POA&M, or quality system, and the contractor shall submit related quality objective evidence upon request. Quality objective evidence (CDRL A014) shall include any of the following as applicable:

- Detailed incoming receipt inspection records
- First article inspection records
- Certificates of Conformance
- Detailed sampling inspection records based upon MIL-STD-1916 (Verification Level III)
- Quality Measurement and Analysis metrics/data

The Government reserves the right to perform any inspections or pull samples as deemed necessary to assure that the contractor provided services, documents, material, and related evidence meet the prescribed requirements and to reject any or all services, documents, and material in a category when nonconformance is established.

6.5 QUALITY MANAGEMENT DOCUMENTATION

In support of the contract's Quality Assurance Surveillance Plan (QASP) and Contractor Performance Assessment Reporting System (CPARS), the contractor shall provide the following documents: Price and Schedule Milestone Plan (CDRL A015) submitted 10 days after Task Order award, and Contractor CPARS Draft Approval Document (CDAD) Report (CDRL A016) submitted monthly.

7.0 DOCUMENTATION AND DELIVERABLES

7.1 CONTRACT DATA REQUIREMENT LISTINGS (CDRLs)

The following CDRL listing identifies the data item deliverables required under this contract and the applicable section of the PWS for which they are required. Section J includes the DD Form 1423s that itemize each Contract Data Requirements List (CDRL) required under the basic contract. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs generated under each task. The contractor shall not develop any CDRL classified TOP SECRET with SCI.

CDRL #	Description	PWS Reference Paragraph	Security Classification (up to S/TS or unclassified)
A001	Program Management Reports, General	3.3.2	Unclassified
A002	Technical/Analysis Reports, General	3.1, 3.2.5.1.2, 3.3.2, 3.4.1.2, 3.4.2.4, 3.4.2.5, 3.4.3, 3.4.4.3, 3.4.5.2, 3.4.5.3*	Secret

CDRL #	Description	PWS Reference Paragraph	Security Classification (up to S/TS or unclassified)
A003	Software Documentation/Programmer's Guide	3.3.2	Unclassified
A004	Training Documentation	3.3.2, 3.5.1.1, 3.5.1.2, 3.5.1.3	Unclassified
A005	Trip Report	3.5.2.5	Unclassified
A006	Contract Status Report (CSR)	5.2.1.1, 8.1.2	Unclassified
A007	Task Order Status Report (TOSR)	5.2.1.2, 8.1.2	Unclassified
A008	Task Order Closeout Report	5.2.1.3	Unclassified
A009	Cyber Security Workforce (CSWF) Report	3.4.6.1(b), 5.2.1.4, 8.1.2	Unclassified
A010	RESERVED		
A011	Invoice Support Documentation	5.2.1.6	Unclassified
A012	RESERVED		
A013	RESERVED		
A014	Quality Documentation	6.1, 6.4	Unclassified
A015	Price and Schedule Milestone Plan	6.5	Unclassified
A016	Contractor CPARS Draft Approval Document (CDAD) Report	6.5	Unclassified
A017	OCONUS Deployment Documentation and Package	14.4	Unclassified
A018	Software Development Plan (SDP)	3.3.2, 3.4.3.6	Unclassified

* PWS Reference (continued) 3.4.6.3.4.1, 3.4.6.3.4.2, 3.4.7.3.1, 3.4.7.5.1, 3.4.7.5.2

7.2 ELECTRONIC FORMAT

At a minimum, the contractor shall provide deliverables electronically by e-mail; hard copies are only required if requested by the Government. To ensure information compatibility, the contractor shall guarantee all deliverables (i.e., CDRLs), data, correspondence, etc., are provided in a format approved by the receiving Government representative. The contractor shall provide all data in an editable format compatible with SPAWARSYSCEN Atlantic corporate standard software configuration as specified below. Contractor shall conform to SPAWARSYSCEN Atlantic corporate standards within 30 days of contract award unless otherwise specified. *The initial or future upgrades costs of the listed computer programs are not chargeable as a direct cost to the Government*.

	Deliverable	Software to be used
a.	Word Processing	Microsoft Word
b.	Technical Publishing	PageMaker/Interleaf/SGML/ MSPublisher
c.	Spreadsheet/Graphics	Microsoft Excel
d.	Presentations	Microsoft PowerPoint
e.	2-D Drawings/ Graphics/Schematics (new data products)	Vector (CGM/SVG)
f.	2-D Drawings/ Graphics/Schematics (existing data products)	Raster (CALS Type I, TIFF/BMP, JPEG, PNG)
g.	Scheduling	Microsoft Project
h.	Computer Aid Design (CAD) Drawings	AutoCAD/Visio
i.	Geographic Information System (GIS)	ArcInfo/ArcView

7.3 INFORMATION SYSTEM

7.3.1 Electronic Communication

The contractor shall have broadband Internet connectivity and an industry standard email system for communication with the Government. The contractor shall be capable of Public Key Infrastructure client side authentication to DOD private web servers. Unless otherwise specified, all key personnel on contract shall be accessible by email through individual accounts during all working hours.

7.3.2 Information Security

Pursuant to DoDM 5200.01, the contractor shall provide adequate security for all unclassified DoD information passing through non-DoD information system including all subcontractor information systems utilized on contract. The contractor shall disseminate unclassified DoD information within the scope of assigned duties and with a clear expectation that confidentiality is preserved. Examples of such information include the following: non-public information provided to the contractor, information developed during the course of the contract, and privileged contract information (e.g., program schedules, contract-related tracking).

7.3.2.1 Safeguards

The contractor shall protect Government information and shall provide compliance documentation validating they are meeting this requirement in accordance with DFARS Clause 252.204-7012. The contractor and all utilized subcontractors shall abide by the following safeguards:

(a) Do not process DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

(b) Protect information by at least one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

(c) Sanitize media (e.g., overwrite) before external release or disposal.

(d) Encrypt all information that has been identified as controlled unclassified information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as portable hard drives and digital optical disks, using DoD Authorized Data-at-Rest encryption technology. NOTE: Thumb drives are not authorized for DoD work, storage, or transfer. Use GSA Awarded DAR solutions (GSA # 10359) complying with ASD-NII/DOD-CIO Memorandum, "Encryption of Sensitive Unclassified Data-at-Rest on Mobile Computing Devices and Removable Storage." The contractor shall ensure all solutions meet FIPS 140-2 compliance requirements.

(e) Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.

(f) Transmit e-mail, text messages, and similar communications using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS). Encrypt organizational wireless connections and use encrypted wireless connection where available when traveling. If encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using at least application-provided password protection level encryption.

(g) Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

(h) Do not post DoD information to Web site pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to Web site pages that control access by user identification or password, user certificates, or other technical means and provide protection via use of TLS or other equivalent technologies. Access control may be provided by the intranet (vice the Web site itself or the application it hosts).

(i) Provide protection against computer network intrusions and data exfiltration, minimally including the following:

1. Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

2. Monitoring and control of inbound and outbound network traffic as appropriate (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

3. Prompt application of security-relevant software patches, service packs, and hot fixes.

(j) As applicable, comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, critical program information (CPI), personally identifiable information, export controlled).

(k) Report loss or unauthorized disclosure of information in accordance with contract or agreement requirements and mechanisms.

7.3.2.2 Compliance

Pursuant to DoDM 5200.01, the contractor shall include in their quality processes procedures that are compliant with information security requirements.

8.0 SECURITY

	Document Number	Title
a..	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08
b.	DoD 5220.22-M	DoD Manual – National Industrial Security Program Operating Manual (NISPOM) dtd 28 Feb 06
c.	DoDI 5220.22	DoD Instruction – National Industrial Security Program dtd 18 Mar 11
d.	DoD 5200.2-R	DoD Regulation – Personnel Security Program dtd Jan 87
e.	DoDD 5205.02E	DoD Directive – Operations Security (OPSEC) Program dtd 20 Jun 12
f.	DoD 5205.02-M	DoD Manual – Operations Security (OPSEC) Program Manual dtd 3 Nov 08
g.	DoDI 5220.22	DoD Instruction – National Industrial Security Program, dtd 18 Mar 11
h.	DoDI 8500.01	DoD Instruction – Cybersecurity dtd 14 Mar 14
i.	DoD 8570.01-M	Information Assurance Workforce Improvement Program dtd 19 Dec 05 with Change 3 dtd 24 Jan 12
j.	SECNAV M-5239.2	DON Information Assurance Workforce Management Manual dtd May 2009
k.	SECNAV M-5510.30	Secretary of the Navy Manual – DoN Personnel Security Program dtd Jun 06
l.	SECNAVINST 5510.30	DoN Regulation – Personnel Security Program
m.	SPAWARINST 3432.1	SPAWAR Instruction – Operations Security (OPSEC) Policy dtd 2 Feb 05
n.	NIST SP 800-Series	National Institute of Standards and Technology Special Publications 800 Series – Computer Security Policies, Procedures, and Guidelines

	Document Number	Title
o.	N/A	SPAWARSYSCEN Atlantic Contractor Checkin portal – https://wiki.spawar.navy.mil/confluence/display/SSCACOG/Contractor+Checkin
p.	HSPD-12	Homeland Security Presidential Directive – Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004
q.	DoDM-1000.13-M-V1	DoD Manual – DoD Identification Cards: ID card Life-Cycle dtd 23 Jan 14
r.	FIPS PUB 201-2	Federal Information Processing Standards Publication 201-2 – Personal Identity Verification (PIV) of Federal Employees and Contractors, August 2013
s.	Form I-9, OMB No. 115-0136	US Department of Justice, Immigration and Naturalization Services, Form I-9, OMB No. 115-0136 – Employment Eligibility Verification

8.1 ORGANIZATION

8.1.1 Security Classification

Classified work shall be performed under this contract and subsequent task orders, as required. The contractor shall have at the time of contract award and prior to commencement of classified work, a SECRET facility security clearance (FCL).

The following PWS task(s) requires access to classified information up to the level of SECRET: 3.1, 3.2, 3.3, 3.4, 3.5.

U.S. Government security clearance eligibility is required to access and handle classified and certain controlled unclassified information (CUI), attend program meetings, and/or work within restricted areas unescorted.

8.1.2 Security Officer

The contractor shall appoint a Facility Security Officer (FSO) to support those contractor personnel requiring access to Government facility/installation and/or access to information technology systems under this contract. The FSO is the contractor's main POC for security issues. The FSO shall have a U.S. Government security clearance equal to or higher than the FCL required on this contract. The FSO shall be responsible for tracking the security requirements for all personnel (subcontractors included) utilized on contract. Responsibilities include entering and updating the personnel security related and mandatory training information within the Staffing Plan document, which is an attachment to the contract/task order status report (CSR/TOSR) (CDRL A006 CDRL A007). FSO shall also update and track data in the Cyber Security Workforce (CSWF) (CDRL A009).

8.2 PERSONNEL

The contractor shall conform to the security provisions of DoDI 5220.22/DoD 5220.22-M – National Industrial Security Program Operating Manual (NISPOM), SECNAVINST 5510.30, DoD 8570.01-M, and the Privacy Act of 1974. Prior to any labor hours being charged on contract, the contractor shall ensure all personnel (including administrative and subcontractor personnel) have obtained and can maintain favorable background investigations at the appropriate level(s) for access required for the contract/task order, and if applicable, are certified/credentialed for the Cybersecurity Workforce (CSWF). A favorable background determination is determined by either a National Agency Check with Inquiries (NACI), National Agency Check with Law and Credit (NACLC), or Single Scope Background Investigation (SSBI) and favorable Federal Bureau of Investigation (FBI) fingerprint checks. Investigations are not necessarily required for personnel performing unclassified work who do not require access to Government installations/facilities, Government IT systems and IT resources, or SPAWARSYSCEN Atlantic information. Cost to meet these security requirements is not directly chargeable to task order.

NOTE: If a final determination is made that an individual does not meet or cannot maintain the minimum security fitness standard, the contractor shall permanently remove the individual from SPAWARSYSCEN Atlantic facilities, projects, and/or programs. If an individual who has been submitted for a fitness determination or security clearance is "denied" or receives an "Interim Declination," the contractor shall remove the individual from SPAWARSYSCEN Atlantic facilities, projects, and/or programs until such time as the investigation is fully adjudicated or the individual is resubmitted and is approved. All contractor and subcontractor personnel removed from facilities, projects, and/or programs shall cease charging labor hours directly or indirectly on task and contract.

8.2.1 Personnel Clearance

The majority of personnel associated with this contract shall possess a SECRET personnel security clearance (PCL). These programs/tasks include, as a minimum, contractor personnel having the appropriate clearances required for access to classified data as applicable. Prior to starting work on the task, contractor personnel shall have the required clearance granted by the Department of Defense Consolidated Adjudications Facility (DoD CAF) and shall comply with IT access authorization requirements. In addition, contractor personnel shall possess the appropriate IT level of access for the respective task and position assignment as applicable per DoDI 8500.01, Cybersecurity. Any future revision to the respective directive and instruction shall be applied to the TO level as required. Contractor personnel shall handle and safeguard any Controlled Unclassified Information (CUI) and/or classified information in accordance with appropriate Department of Defense, Navy, and SPAWARSYSCEN Atlantic security regulations. The contractor shall immediately report any security violation to the SPAWARSYSCEN Atlantic Security Management Office, the COR, and the Government Project Manager.

8.2.2 Access Control of Contractor Personnel

8.2.2.1 Physical Access to Government Facilities and Installations

Contractor personnel shall physically access Government facilities and installations for purposes of site visitation, supervisory and quality evaluation, work performed within Government spaces (either temporary or permanent), or meeting attendance. Individuals supporting these efforts shall comply with the latest security regulations applicable to the Government facility/installation.

(a) The majority of Government facilities require contractor personnel to have an approved visit request on file at the facility/installation security office prior to access. The contractor shall initiate and submit a request for visit authorization to the COR in accordance with DoD 5220.22-M (NISPOM) not later than one (1) week prior to visit – timeframes may vary at each facility/ installation. For admission to SPAWARSYSCEN Atlantic facilities/installations, the contractor shall forward a visit request to Joint Personnel Adjudication System (JPAS) /SMO 652366; faxed to 843-218-4045 or mailed to Space and Naval Warfare Systems Center Atlantic, P.O. Box 190022, North Charleston, SC 29419-9022, Attn: Security Office, for certification of need to know by the specified COR. For visitation to all other govt. locations, the contractor shall forward visit request documentation directly to the on-site facility/installation security office (to be identified at task order level) via approval by the COR.

(b) Depending on the facility/installation regulations, contractor personnel shall present a proper form of identification(s) and vehicle proof of insurance or vehicle rental agreement. NOTE: SPAWARSYSCEN Atlantic facilities located on Joint Base Charleston require a Common Access Card (CAC) each time physical installation access is required. Contractor shall contact SPAWARSYSCEN Atlantic Security Office directly for latest policy.

(c) All contractor persons engaged in work while on Government property shall be subject to inspection of their vehicles at any time by the Government, and shall report any known or suspected security violations to the Security Department at that location

8.2.2.2 Identification and Disclosure Requirements

Pursuant to DFARS 211.106, Contractors shall take all means necessary to not represent themselves as Government employees. All Contractor personnel shall follow the identification and disclosure requirement as specified in local clause 5252.237-9602. In addition, contractor and subcontractors shall identify themselves and their company name on attendance meeting list/minutes, documentation reviews, and their electronic digital signature.

8.2.2.3 Government Badge Requirements

As specified in contract clause 5252.204-9202, some contract personnel shall require a Government issued picture badge. While on Government installations/facilities, contractors shall abide by each site's security badge requirements. Various Government installations are continually updating their security requirements to meet Homeland Security Presidential Directive (HSPD-12) identification standards. Contractors are responsible for obtaining and complying with the latest security identification requirements for their personnel as required. Contractors shall submit valid paper work (e.g., site visit request, request for picture badge, and/or SF-86 for Common Access Card (CAC)) to the applicable Government security office via the contract COR. The contractor's appointed Security Officer shall track all personnel holding local Government badges at contract or TO level.

8.2.2.4 Common Access Card (CAC) Requirements

Some Government facilities/installations (e.g., Joint Base Charleston) require contractor personnel to have a Common Access Card (CAC) for physical access to the facilities or installations. Contractors supporting work that requires access to any DoD IT/network also requires a CAC. Granting of logical and physical access privileges remains a local policy and business operation function of the local facility. The Contractor is responsible for obtaining the latest facility/installation and IT CAC requirements from the applicable local Security Office. When a CAC is required to perform work, contractor personnel shall be able to meet all of the following security requirements prior to work being performed:

(a) Pursuant to DoD Manual (DoDM-1000.13-M-V1), issuance of a CAC is based on the following four criteria:

1. Eligibility for a CAC – to be eligible for a CAC, Contractor personnel's access requirement shall meet one of the following three criteria: (a) individual requires access to multiple DoD facilities or access to multiple non-DoD Federal facilities on behalf of the Government on a recurring bases for a period of 6 months or more, (b) individual requires both access to a DoD facility and access to DoD network on site or remotely, or (c) individual requires remote access to DoD networks that use only the CAC logon for user identification.
2. Verification of DoD affiliation from an authoritative data source – CAC eligible personnel must be registered in the Defense Enrollment Eligibility Reporting Systems (DEERS) through either an authoritative personnel data feed from the appropriate Service or Agency or Trusted Associated Sponsorship System (TASS) (formally Contractor Verification System (CVS)).
3. Completion of background vetting requirements according to FIPS PUB 201-2 and DoD Regulation 5200.2-R – at a minimum, the completion of Federal Bureau of Investigation (FBI) fingerprint check with favorable results and submission of a National Agency Check with Inquiries (NACI) investigation to the Office of Personnel Management (OPM), or a DoD-determined equivalent investigation. NOTE: Contractor personnel requiring logical access shall obtain and maintain a favorable National Agency Check with Law and Credit (NACLC) investigation. Contractor personnel shall contact the SPAWARSYSCEN Atlantic Security Office to obtain the latest CAC requirements and procedures.
4. Verification of a claimed identity – all contractor personnel shall present two forms of identification in its original form to verify a claimed identity. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 115-0136, Employment Eligibility Verification. Consistent with applicable law, at least one document from the Form I-9 list must be a valid (unexpired) State or Federal Government-issued picture identification (ID). The identity documents will be inspected for authenticity, scanned, and stored in the DEERS.

(b) When a contractor requires logical access to a Government IT system or resource (directly or indirectly), the required CAC will have a Public Key Infrastructure (PKI). A hardware solution and software (e.g., ActiveGold) is required to securely read the card via a personal computer. Pursuant to DoDM 1000.13-M-V1, CAC PKI certificates will be associated with an official Government issued e-mail address (e.g. .mil, .gov, .edu). Prior to receipt of a CAC with PKI, contractor personnel shall complete the mandatory Cybersecurity Awareness training and submit a signed System Authorization Access Request Navy (SAAR-N) form to the contract's specified COR. Note: In order for personnel to maintain a CAC with PKI, each contractor employee shall complete annual cybersecurity training. The following guidance for training and form submittal is provided; however, contractors shall seek latest guidance from their appointed company Security Officer and the SPAWARSYSCEN Atlantic Information Assurance Management (IAM) office:

1. For annual DoD Cybersecurity/IA Awareness training, contractors shall use this site: https://twms.nmci.navy.mil/. For those contractors requiring initial training and do not have a CAC, contact the SPAWARSYSCEN Atlantic IAM office at phone number (843)218-6152 or e-mail questions to ssc_lant_iam_office.fcm@navy.mil for additional instructions. Training can be taken at the IAM office or online at http://iase.disa.mil/index2.html.
2. For SAAR-N form, the contractor shall use OPNAV 5239/14 (Rev 9/2011). Contractors can obtain a form from the SPAWARSYSCEN Atlantic IAM office at or from the website: https://navalforms.documentservices.dla.mil/. Digitally signed forms will be routed to the IAM office via encrypted e-mail to ssclant_it_secmtg@navy.mil.

8.2.2.5 Contractor Check-in and Check-out Procedures

All SPAWARSYSCEN Atlantic contractor personnel requiring or possessing a Government badge and/or CAC for facility and/or IT access shall have a SPAWARSYSCEN Atlantic Government sponsor and be in compliance with the most current version of Contractor Check-in and Check-out Instruction and Forms as posted on the Command Operating Guide (COG) website. At contract award throughout contract completion, the contractor shall provide necessary employee information and documentation for employees hired, transferred, and/or terminated in support of this contract within the required timeframe as cited in the Check-in and Check-out instructions. Contractor's Security Officer shall ensure all contractor employees whose services are no longer required on contract return all applicable Government documents/badges to the appropriate Government representative. NOTE: If the contractor does not have access to the SPAWAR COG website, the contractor shall get all necessary instruction and forms from the COR.

8.2.3 IT Position Categories

Pursuant to DoDI 8500.01, DoD 8570.01-M, SECNAVINST 5510.30, SECNAV M-5239.2, and applicable to unclassified DoD information systems, a designator is assigned to certain individuals that indicates the level of IT access required to execute the responsibilities of the position based on the potential for an individual assigned to the position to adversely impact DoD missions or functions. As defined in DoD 5200.2-R, SECNAVINST 5510.30 and SECNAV M-5510.30, three basic DoN IT levels/Position categories exist:

- IT-I (Privileged access)
- IT-II (Limited Privileged, sensitive information)
- IT-III (Non-Privileged, no sensitive information)

Note: The term IT Position is synonymous with the older term Automated Data Processing (ADP) Position (as used in DoD 5200.2-R, Appendix 10).

Investigative requirements for each category vary, depending on the role and whether the individual is a U.S. civilian contractor or a foreign national. The Contractor PM shall assist the Government Project Manager or COR in determining the appropriate IT Position Category assignment for all contractor personnel. All required Single-Scope Background Investigation (SSBI), SSBI Periodic Reinvestigation (SSBI-PR), and National Agency Check (NAC) adjudication will be performed Pursuant to DoDI 8500.01 and SECNAVINST 5510.30. Requests for investigation of contractor personnel for fitness determinations or IT eligibility without classified access are submitted by SPAWARSYSCEN Atlantic Security Office, processed by the OPM, and adjudicated by DOD CAF. IT Position Categories are determined based on the following criteria:

8.2.3.1 IT-I Level (Privileged) - Positions in which the assigned individual is responsible for the planning, direction, and implementation of a computer security program; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain. Personnel whose duties meet the criteria for IT-I Position designation require a favorably adjudication of Single Scope Background Investigation (SSBI) or SSBI-PR. The SSBI or SSBI-PR is updated a minimum of every 5 years. Assignment to designated IT-I positions requires U.S. citizenship unless a waiver request is approved by CNO.

8.2.3.2 IT-II Level (Limited Privileged) - Positions in which the assigned individual is responsible for the-direction, planning, design, operation, or maintenance of a computer system, and whose work is technically

reviewed by a higher authority at the IT-II Position level to insure the integrity of the system. Personnel whose duties meet the criteria for an IT-II Position require a favorably adjudication of a Position of Trust National Agency Check with Law and Credit (PT/NACLC). Assignment to designated IT-II positions requires U.S. citizenship unless a waiver request is approved by CNO.

8.2.3.3 IT-III Level (Non-privileged) - All other positions involved in computer activities. Assigned individual in this position has non-privileged access to one or more DoD information systems/applications or database to which they are authorized access. Personnel whose duties meet the criteria for an IT-III Position designation require a favorably adjudication of a Position of Trust National Agency Check with Written Inquiries (PT/NACI).

8.2.4 Security Training

Regardless of the contract security level required, the contractor shall be responsible for verifying applicable personnel (including subcontractors) receive all required training. At a minimum, the contractor's designated Security Officer shall track the following information: security clearance information; dates possessing Common Access Cards; issued & expired dates for SPAWARSYSCEN Atlantic Badge; Cybersecurity training; Privacy Act training; Personally Identifiable Information (PII) training; Cybersecurity Workforce (CSWF) certifications; etc. The contractor shall educate employees on the procedures for the handling and production of classified material and documents, and other security measures as described in the PWS in accordance with DoD 5220.22-M.

8.2.5 Disclosure of Information

In support of DFARS Clause 252.204-7000, contractor employees shall not discuss or disclose any information provided to them in the performance of their duties to parties other than authorized Government and contractor personnel who have a "need to know". The contractor shall not use any information or documentation developed by the contractor under direction of the Government for other purposes without the consent of the Government Contracting Officer.

8.2.6 Handling of Personally Identifiable Information (PII)

When a contractor, including any subcontractor, is authorized access to Personally Identifiable Information (PII), the contractor shall complete annual PII training requirements and comply with all privacy protections under the Privacy Act (Clause 52.224-1 and 52.224-2). The contractor shall safeguard PII from theft, loss, and compromise. The contractor shall transmit and dispose of PII in accordance with the latest DON policies. The contractor shall not store any Government PII on their personal computers. The contractor shall mark all developed documentation containing PII information accordingly in either the header or footer of the document: "FOUO – Privacy Sensitive. Any misuse or unauthorized disclosure may result in both criminal and civil penalties." Any unauthorized disclosure of privacy sensitive information through negligence or misconduct can lead to contractor removal or contract termination depending on the severity of the disclosure. Upon discovery of a PII breach, the contractor shall immediately notify the Contracting Officer and COR. Contractors responsible for the unauthorized disclosure of PII shall be held accountable for any costs associated with breach mitigation, including those incurred as a result of having to notify personnel.

8.3 OPERATIONS SECURITY (OPSEC) REQUIREMENTS

Security programs are oriented towards protection of classified information and material. Operations Security (OPSEC) is an operations function which involves the protection of any critical information – focusing on unclassified information that may be susceptible to adversary exploitation. Pursuant to DoDD 5205.02E and SPAWARINST 3432.1, SPAWARSYSCEN Atlantic's OPSEC program implements requirements in DoD 5205.02-M – OPSEC Program Manual. Note: OPSEC requirements are applicable when contract personnel have access to either classified information or unclassified Critical Program Information (CPI)/sensitive information.

8.3.1 Local and Internal OPSEC Requirement

Contractor personnel, including subcontractors if applicable, shall adhere to the OPSEC program policies and practices as cited in the SPAWARINST 3432.1 and existing local site OPSEC procedures. The contractor shall development their own internal OPSEC program specific to the contract and based on SPAWARSYSCEN Atlantic

OPSEC requirements. At a minimum, the contractor's program shall identify the current SPAWARSYSCEN Atlantic site OPSEC Officer/Coordinator.

8.3.2 OPSEC Training

Contractor shall track and ensure applicable personnel receive initial and annual OPSEC awareness training. Training may be provided by the Government or a contractor's OPSEC Manager. Contractor training shall, as a minimum, cover OPSEC as it relates to contract work, discuss the Critical Information applicable in the contract/task order, and review OPSEC requirements if working at Government facilities. The contractor shall ensure any training materials developed by the contractor shall be reviewed by the SPAWARSYSCEN Atlantic OPSEC Officer, who will ensure it is consistent with SPAWARSYSCEN Atlantic OPSEC policies. OPSEC training requirements are applicable for personnel during their entire term supporting SPAWAR contracts.

8.3.3 SPAWARSYSCEN Atlantic OPSEC Program

Contractor shall participate in SPAWARSYSCEN Atlantic OPSEC program briefings and working meetings and the contractor shall complete any required OPSEC survey or data call within the timeframe specified.

8.3.4 Classified Contracts

OPSEC requirements identified under a classified contract shall have specific OPSEC requirements listed on the DD Form 254.

8.4 DATA HANDLING AND USER CONTROLS

8.4.1 Data Handling

At a minimum, the contractor shall handle all data received or generated under this contract as For Official Use Only (FOUO) material. Any classified information received or generated shall be handled in accordance with the attached DD Form 254 and in shall be in compliance with all applicable PWS references and to other applicable Government policies and procedures that include DOD/Navy/SPAWAR.

8.4.2 Effective Use of Controls

The contractor shall screen all electronic deliverables or electronically provided information for malicious code using DoD approved anti-virus software prior to delivery to the Government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect contract related information processed, stored or transmitted on the contractor's and Government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. The contractor shall ensure provisions are in place that will safeguard all aspects of information operations pertaining to this contract in compliance with all applicable PWS references. In compliance with Para 7.3.2.1, the contractor shall ensure Data-at-Rest is required on all portable electronic devices including storage of all types. Encryption/digital signing of communications is required for authentication and non-repudiation.

9.0 GOVERNMENT FACILITIES

As specified in each task order, Government facilities (i.e., office space, computer hardware/software, or lab space) will be provided to those labor categories that would otherwise adversely affect the work performance if they were not available on-site. All Contractor personnel with supplied Government facilities shall be located at SPAWARSYSCEN Atlantic in Charleston, SC. Note: *The burdened labor rate for those contractor personnel designated as "Government site" shall include overhead costs allocable to Government site work, consistent with the contractor's established accounting practices*.

10.0 CONTRACTOR FACILITIES

As specified in each task order, the contractor shall have facilities (i.e., office space, laboratory space, staging and storage areas, with or without classified storage) in order to accomplish task order objectives.

11.0 CONTRACT PROPERTY ADMINISTRATION

No Government property will be provided or acquired on this contract or any subsequent task order.

12.0 SAFETY ISSUES

12.1 OCCUPATIONAL SAFETY AND HEALTH REQUIREMENTS

The contractor shall be responsible for ensuring the safety of all company employees, other working personnel, and Government property. The contractor is solely responsible for compliance with the Occupational Safety and Health Act (OSHA) (Public Law 91-596) and the resulting applicable standards, OSHA Standard 29 CFR 1910 (general), 1915 (shipboard/submarine) and 1926 (shore), and for the protection, safety and health of their employees and any subcontractors assigned to the respective task orders under this contract. Without Government assistance, the contractor shall make certain that all safety requirements are met, safety equipment is provided, and safety procedures are documented as part of their quality management system.

12.1.1 Performance at Government facilities

The contractor shall immediately report any accidents involving Government or contractor personnel injuries or property/equipment damage to the contracting officer and COR. Additionally, the contractor is responsible for securing the scene and impounding evidence/wreckage until released by the contracting officer.

12.2 SAFETY TRAINING

The contractor shall be responsible to train all personnel that require safety training. Specifically, where contractors are performing work at Navy shore installations, that requires entering manholes or underground services utility the contractor shall provide a qualified person as required in 29 CFR 1910 or 29 CFR 1926 or as recommended by the National Institute for Occupational Safety and Health (NIOSH) Criteria Document for Confined Spaces. Also, when contractors are required to scale a tower, all applicable personnel shall have Secondary Fall Protection and Prevention training.

13.0 SMALL BUSINESS SUBCONTRACTING PLAN

In accordance with FAR clause 52.219-9, the contractor shall effectively implement their Government approved Small Business Subcontracting Plan throughout the life of the contract. The contractor shall provide for maximum practicable opportunity for Small Business to participate in contract performance consistent with efficient contract performance. The contractor shall demonstrate or at least document they have provided their best attempt to meet all terms and conditions in the contract relating to Small Business participation. Inability to adhere to an effective subcontracting program shall negatively affect a contractor's annual Government Contractor Performance Assessment Report (CPAR) rating.

14.0 TRAVEL

14.1 LOCATIONS

If travel is required at the task order level, the contractor shall be prepared to travel to the following locations:

1) Charleston, SC
2) Okinawa, JP
3) Iwakuni, JP
4) Camp Lejeune, NC
5) Cherry Point, NC

6) Camp Pendleton, CA
7) Miramar, CA
8) Kaneohe Bay, HI
9) Oahu, HI
10) Quantico, VA
11) Dam Neck, VA

Note: Under this contract and any subsequent task orders, the contractor shall not travel to Afghanistan.

14.2 PERSONNEL MEDICAL REQUIREMENTS

14.2.1 OCONUS Immunization Requirements

As specified in each task order, the contractor shall be required to travel to locations outside the Continental limits of the United States (OCONUS) both shore and afloat. Contractor employees who deploy to locations that require immunizations shall do so pursuant to DoDI 6205.4, Department of the Navy (DON), and SPAWARSYSCENLANTINST 12910.1A.

14.3 LETTER OF AUTHORIZATION

Some travel will require a Letter of Authorization (LOA). As noted in DFARS PGI 225.7402-3(e), an LOA is necessary to enable a contractor employee to process through a deployment processing center; to travel to, from, and within a theater of operations; and to identify any additional authorizations and privileges. Applicable to the task order, the contractor shall initiate an LOA for each prospective traveler. The contractor shall use the Synchronized Pre-deployment & Operational Tracker (SPOT) web-based system, at http://www.dod.mil/bta/products/spot.html, to enter and maintain data with respect to traveling/deployed personnel, and to generate LOAs. When necessary and if in the Government's interest, the contractor may also initiate an LOA request to provide an official traveler access to Government facilities and to take advantage of travel discount rates in accordance with Government contracts and/or agreements. All privileges, services, and travel rate discount access are subject to availability and vendor acceptance. LOAs are required to be signed/approved by the SPOT registered Contracting/Ordering Officer for the applicable contract/task order.

Note for travel to Iraq: The only acceptable LOAs for work performed in Iraq are in support of Office of Security Cooperation - Iraq (OSC-I) or the Dept. of State (DoS). Support in reference to U.S. Forces Iraq (USF-I) is no longer valid beyond Dec 2011.

14.4 SPECIFIED MISSION DESTINATIONS

As specified in each task order, the contractor shall be required to travel to locations designated as Specified Mission Destinations which are listed in the latest SPAWARSYSCEN Atlantic OCONUS Travel Guide portal (latest link to be provided at contract and task order award). Pursuant to DoDI 3020.41 and SPAWARSYSCENLANTINST 12910.1A, work to be performed at Specified Mission Destinations is subject to all relevant contract clauses, as well as the requirements set forth in the aforementioned guide. The contractor shall be able to meet all clause and guide requirements 35 days prior to travel within the applicable specified destinations. When deployment to a Specified Mission Destination is required, the contractor shall be responsible for processing applicable deployment packages for its personnel in accordance with the SPAWARSYSCEN Atlantic OCONUS Travel Guide portal. Note: The portal is NOT the authoritative source, as it is only a guide. The contractor shall be responsible to know and understand travel requirements as identified by the Combatant Command (COCOM) and applicable country. Commencing no later than seven (7) days after task order award requiring travel to specified mission destination(s), the contractor shall submit all required OCONUS Deployment Documentation and Package (CDRL A017) to the task order technical POC and/or Command Travel/Deployment Coordinator.

CLAUSES INCORPORATED BY FULL TEXT

5252.216-9217, ALT II DELIVERY/TASK ORDER PROCEDURES (MAY 2009), ALTERNATE II

(a) *Procedures*. Each delivery/task order shall be placed in accordance with the following procedures:

(1) Upon identification of a requirement, the Contracting Officer's Representative (COR) or originator shall contact the Contractor for the purpose of arriving at a common understanding of the technical components which constitute the basis for performance under this delivery/task order and identifying the elements necessary for preparing a detailed Statement of Work (SOW) which contains sufficient definition to allow all parties to clearly identify an end product consistent with the scope of the contract.

(2) After both parties have reached agreement regarding the technical requirement of the SOW, and the SOW is completed, the Contractor and the COR shall sign and date the document to signify their common understanding of the delivery/task order requirements.

(3) Within five (5) calendar days after signing the SOW, the Contractor shall submit to the Ordering Officer/Administrator a complete price estimate, with a copy of the SOW attached for the delivery/task order, sufficient to adequately describe how the Contractor will complete the requirements of the SOW. A copy of the price estimate shall be forwarded concurrently to the COR and/or originator. The price estimate shall contain the following documentation to enable the Ordering Officer/Administrator to make a determination of price reasonableness:

(A) CLIN, Quantity, Unit Price, Amount
(B) Labor Category (CLINS 0004 and 0009 only)
(C) Number of Hours (CLINS 0004 and 0009 only)
(D) Other Direct Costs (ODCs) (CLIN 0012)

1. Travel identified in the SOW needs only a total price. Travel requirements not identified in the SOW must be fully documented including destination, number of people, number of days, airfare, per diem, car rental and other charges.

2. Material exceeding a unit price in excess of the micro purchase threshold per FAR 2.101 must be itemized. All other materials need only a total price.

3. Equipment must be identified as Information Technology (IT) or non-IT. All IT equipment must be itemized. Non-IT equipment exceeding a unit price in excess of the micro purchase threshold per FAR 2.101 must be itemized. All other equipment not identified above needs only a total price.

4. Total miscellaneous charges under the micro purchase threshold per FAR 2.101 do not need to be itemized.

(E) Subcontractors (CLINS 0004 and 0009 only)

Any backup documentation not provided when you submit your price estimate may be requested later by the Ordering Officer.

*NOTE: If the proposal is based on a labor hour contract, no material costs will be authorized.

(4) Once the Ordering Officer/Administrator has reviewed and accepted the Contractor's price estimate, a DD Form 1155 will be executed by the Contracting Officer/Ordering Officer and sent to the Contractor as notice to begin work. The Contractor is cautioned that no work is to be started prior to receipt of a properly signed and executed DD Form 1155, Order for Supplies/Services. If the price estimate is insufficient or discussions are needed, the administrator will contact the Contractor to negotiate requirements.

(5) Delivery or task orders may be issued under this contract by facsimile or by electronic commerce methods.

(b) *Content and Effect.*

Each delivery/task order shall include:
(i) Effective date of order,
(ii) Contract and delivery/task order numbers,
(iii) CLIN, quantity, unit price, and amount

(iv) Place of delivery or performance,
(v) Scope, including reference to applicable (contract) specifications,
(vi) Place and manner of inspection and acceptance, if different from that specified in the basic contract,
(vii) An estimate of the number of hours of labor and labor rate required to perform the order (CLINS 0004 and 0009 only)
(viii) A ceiling price,
(ix) Delivery date or period of performance,
(x) Accounting and appropriation data,
(xi) Any other information deemed necessary for the performance of the order.

(c) *Maintenance of Records.* The Contractor shall maintain the following cost records under this contract as a minimum:
Records for each delivery/task order, indicating the number of hours of direct labor performed for the FFP-LOE CLINs (0004 and 0009), segregated to the individual employee performing the work,

(d) *Contractor Notification.* (1) The Contractor is responsible for immediately notifying the Ordering Officer/Administrator of any difficulties in performing in accordance with the terms of the order.

(End of clause)

5252.222-9200 WORKWEEK (APR 2012) ALTERNATE I (DEC 2013)

(a) All or a portion of the effort under this contract will be performed on a Government installation. The normal workweek for Government employees at Space and Naval Warfare Systems Center Atlantic is Monday through Friday, 7:30 am – 4:00 pm (8 hours per day). Work at this Government installation, shall be performed by the contractor within the normal workweek unless differing hours are specified on the individual task orders. Following is a list of holidays observed by the Government:

Name of Holiday	Time of Observance
New Year's Day	1 January
Martin Luther King Jr. Day	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	4 July
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veteran's Day	11 November
Thanksgiving Day	Fourth Thursday in November
Christmas Day	25 December

(b) If any of the above holidays occur on a Saturday or a Sunday, then such holiday shall be observed by the Contractor in accordance with the practice as observed by the assigned Government employees at the using activity.

(c) If the Contractor is prevented from performance as the result of an Executive Order or an administrative leave determination applying to the using activity, such time may be charged to the contract as direct cost provided such charges are consistent with the Contractor's accounting practices.

(d) This contract does not allow for payment of overtime during the normal workweek for employees who are not exempted from the Fair Labor Standards Act unless expressly authorized by the Ordering Officer. Under Federal regulations the payment of overtime is required only when an employee works more than 40 hours in a normal week period.
(e) NOTICE: All Contractor employees who make repeated deliveries to military installations shall obtain the required employee pass via the Navy Commercial Access Control System (NCACS) in order to gain access to the

facility. Information about NCACS may be found at the following website: http://www.cnic.navy.mil/navycni/groups/public/@hq/@cacpmo/documents/document/cnicp_a230767.ppt.

Contractor employees must be able to obtain a NCACS in accordance with base security requirements. Each employee shall wear the Government issued NCACS badge over the front of the outer clothing. When an employee leaves the Contractor's employ, the employee's NCACS pass shall be returned to the Contracting Officer's Representative or the base Badge and Pass Office within five (5) calendar days.

Contractors who do not have a NCACS or Common Access Card (CAC) must be issued a one-day pass daily at the Badge and Pass Office. Issuance of a CAC requires the need for physical access to the installation and logical access to government owned computer systems.

(f) Periodically the Government may conduct Anti-Terrorism Force Protection (AT/FP) and/or safety security exercises which may require the Contractor to adjust its work schedule and/or place of performance to accommodate execution of the exercise. The Contractor will be required to work with its Government point of contact to adjust work schedules and/or place of performance in the case of an exercise that causes disruption of normally scheduled work hours, or disruption of access to a government facility. The contract does not allow for payment of work if schedules cannot be adjusted and/or the work cannot be executed remotely (i.e., the contractor's facility or alternate non-impacted location), during an exercise when government facilities are inaccessible.

(End of clause)

5252.228-9200 LIABILITY INSURANCE--FIXED PRICE CONTRACTS (OCT 2001)

(a) The following types of insurance are required in accordance with the FAR 52.228-5 “Insurance--Work on a Government Installation” clause and shall be maintained in the minimum amounts shown:

(1) Workers’ compensation and employers’ liability: minimum of $100,000

(2) Comprehensive general liability: $500,000 per occurrence

(3) Automobile liability: $200,000 per person
$500,000 per occurrence
$ 20,000 per occurrence for property damage

(b) Upon notification of contract award, the contractor shall furnish to the Contracting Officer, as required by paragraph (b) of the FAR 52.228-5 “Insurance--Work on a Government Installation” clause, a certificate or written statement of insurance prior to commencement of work under this contract. The written statement of insurance must contain the following information: policy number, policyholder, carrier, amount of coverage, dates of effectiveness (i.e., performance period), and contract number. The contract number shall be cited on the certificate of insurance.

(End of clause)

5252.237-9600 PERSONNEL QUALIFICATIONS (MINIMUM) (JAN 1992)

(a) Personnel assigned to or utilized by the Contractor in the performance of this contract shall, as a minimum, meet the experience, educational, or other background requirements set forth below and shall be fully capable of performing in an efficient, reliable, and professional manner. If the offeror does not identify the labor categories

listed below by the same specific title, then a cross-reference list should be provided in the offeror's proposal identifying the difference.

(b) If the Ordering Officer questions the qualifications or competence of any persons performing under the contract, the burden of proof to sustain that the persons is qualified as prescribed herein shall be upon the contractor.

(c) The Contractor must have personnel, organization, and administrative control necessary to ensure that the services performed meet all requirements specified in delivery orders. The work history of each Contractor employee shall contain experience directly related to the tasks and functions to be assigned. The Ordering Officer reserves the right to determine if a given work history contains necessary and sufficiently detailed, related experience to reasonably ensure the ability for effective and efficient performance.

ALLOWABLE LABOR CATEGORIES AND KEY LABOR CATEGORY DESIGNATION

The table below outlines the required labor categories that must be proposed under this contract. Offerors are not permitted to deviate from the hours and labor categories outlined below; however, as outlined in section L, provision L-328, offerors may propose additional labor categories and estimated hours that will be a direct cost based on the offeror's accounting procedures (e.g. management and administrative labor costs).

Key Labor Categories are also identified to establish the Key Personnel:

#	**Labor Category**	**Key Labor Category**
1	Program Manager	X
2	Engineer/Scientist 5	X
3	Engineer/Scientist 4	X
4	Engineer/Scientist 3	
5	Technical Analyst 1	
6	Operations Specialist	
7	Training Specialist 4	
	Service Contract Labor Standards – Wage Determination Categories	
8	Computer Programmer II (14072)	
9	Computer Systems Analyst II (14102)	
10	Computer Systems Analyst III (14103)	

For educational and experience requirements, the following criteria are applicable:

Note 1 To ensure that postsecondary education possessed by individuals meet an acceptable level of quality, educational degrees shall come from accredited institutions or programs. See www.ed.gov for more accreditation information. At a minimum, to receive credit for a Master's and Doctorate, all degrees shall come from an institution that has been regionally accredited by one of the six associations: MSA, NASC, NCA, NEASC, SACS, and WASC.

Note 2 Bachelors of Science (BS) or Associate's (AS) degrees in Applied Science, Computing, Engineering, and Technology shall be from an Accreditation Board for Engineering and Technology (ABET) accredited program (see www.abet.org).

Note 3 When not specified, higher education above a labor category's minimum can be credited as years of experience as long as the higher degree is within the same required field of study as the minimum degree required. The following Educational credit applies: a MS degree equals four (4) years of experience and a PhD degree equals five (5) years of experience.

Note 4 Technology degrees do not qualify as Engineering or Physical Science Degrees.

Note 5 SCLS titles and reference numbers are in accordance with Contract Act Directory of Occupations (Fifth Edition), published in www.dol.gov.

Note 7 ***FOR LOGISTICS LABOR CATEGORIES ONLY*** - DAWIA Certification for Contractors – Contractor personnel that do not have government DAWIA certification courses may demonstrate an equivalency in terms of academic degrees, courses completed, and experience as that of their counterparts in the DAWIA workforce. Equivalency for the following classes must be provided as follows: **Level 1** - (1) Fundamentals of Systems Acquisition Management, (2) Acquisition Logistics Fundamentals, (3) Fundamentals of Systems Sustainment Management, (4) Reliability, Availability and Maintainability (RAM), (5) Designing for Supportability in DoD Systems, (6) Performance Based Life Cycle Product Support (PBL), (7) Fundamentals of Systems Planning, Research, Development, and Engineering; **Level 2** - (1) Level 1 classes, (2) Intermediate Systems Acquisition, (3) Intermediate Acquisition Logistics, (4) Intermediate Systems Sustainment Management, (5) Performance Based Logistics, (6) Life Cycle Management & Sustainment Metrics, (7) Supportability Analysis; **Level 3** - (1) Level 1 and 2 Classes, (2) Life Cycle Product Support, (3) Enterprise Life Cycle Logistics Management, (4) Developing a Life Cycle Sustainment Plan (LCSP), (5) Product Support Business Case Analysis (BCA), (6) Independent Logistics Assessment, AND ONE OF THE FOLLOWING: (a) Mission-Focused Services Acquisition, (b) Operating and Support Cost Analysis, (c) Configuration Management, (d) Core Concepts for Requirements Management. Additional explanation of courses or requirements can be found at the Defense Acquisition University web site (http://icatalog.dau.mil/onlinecatalog/CareerLvl.aspx).

Note 8 ***FOR IA/IW LABOR CATEGORIES ONLY PERFORMING WORK FOR DOD*** – Contractor personnel supporting IA functions shall be certified prior to being engaged in IA related work and be in full compliance with DoD 8570.1-M and DoDD 8570.1 This includes personnel being certified/accredited at the appropriate levels of IAT I-III and IAM I-III as appropriate. This will be verified by the contracting officer who will ensure that contractor personnel are entered in to the Defense Eligibility Enrollment System (DEERS) or other appropriate database. Contractor personnel not certified within 6 months of assignment of IA duties or who fail to maintain their certified status will not be permitted to carry out the responsibilities of the position, and shall be replaced with a contractor who does meet the minimum certification requirements as mandated above.

DEFINITIONS

1. *Relevant Technical Field*, e.g. Electrical Engineering, Computer Science.
2. *Additional Acceptable Degree Fields*, e.g. Management Information Systems.
3. *Specific Projects*, e.g. SINCGARS, DAMA.

The following lists the applicable contract labor categories with their corresponding minimum personnel qualifications:

1. Program Manager

Education: Bachelor's degree in Engineering/Technology (Accredited University), Physical Sciences, Mathematics, Management Information Systems, or Business.

Experience: Fifteen (15) years of technical experience in support of an intelligence program, to include: System Software Integration, Software Testing, Information Assurance, Fielding/Training, and Programmatic Support. Eight (8) years Program Management Experience, to include: Technology Assessments, Systems Design, Systems Analysis, Programmatic Support, Acquisition Planning, and Budget Planning. Knowledge of Federal Acquisition Regulation (FAR) and Department of Defense (DOD) procurement policies and procedures.

2. Engineer/Scientist 5

Education: BS degree in Electrical, Software, Systems or Mechanical Engineering; Physics; Computer Science; or Math.

Software Engineer only: Completed the following certifications within one and a half year after assuming duties: Certified Software Development Professional (CSDP) (Previously known as Certified Software Engineering Professional (CSEP)), or with COR approval complete a vendor/platform specific certification (e.g., Microsoft Certified Solutions Developer (MCSD), Microsoft Certified Applications Developer (MCAD), Microsoft Certified Database Administrator (MCDBA), Red Hat Certification Program (RHCP), CISCO Certified Network Professional (CCNP), Oracle Certified Professional (OCP), other).

Experience: Fifteen (15) years of experience in support of Command, Control, Communications, Combat Systems, Intelligence, Surveillance, and Reconnaissance (C5ISR) systems/equipment, to include: Technology Analysis and Assessment, Design Definition, Development of Software Specifications, Systems Analysis, Systems and Software Architecture, Software Integration and Development, T&E Criteria, and Logistics support of C5ISR requirements. Recognized as an expert in system software design, development, installation and T&E.

3. **Engineer/Scientist 4**

Education: BS degree in Electrical, Software, Systems or Mechanical Engineering; Physics; Computer Science; or Math.
Software Engineer only: Working towards the following certifications within one and a half year after assuming duties: Certified Software Development Professional (CSDP) (Previously known as Certified Software Engineering Professional (CSEP)), or with COR approval complete a vendor/platform specific certification (e.g., Microsoft Certified Solutions Developer (MCSD), Microsoft Certified Applications Developer (MCAD), Microsoft Certified Database Administrator (MCDBA), Red Hat Certification Program (RHCP), CISCO Certified Network Professional (CCNP), Oracle Certified Professional (OCP), other).
Experience: Ten (10) years of experience in support of C5ISR systems/equipment, to include: Technology Analysis and Assessment, Design Definition, Development of Software Specifications, Systems Analysis, Systems and Software Architecture, Software Integration and Development, T&E Criteria, and Logistics support of C5ISR requirements. Note: Experience may be concurrent.

4. **Engineer/Scientist 3**

Education: BS degree in Electrical, Software, Systems or Mechanical Engineering; Physics; Computer Science; or Math.
Software Engineer only: Working towards the following certifications within one and a half year after assuming duties: Certified Software Development Professional (CSDP) (Previously known as Certified Software Engineering Professional (CSEP)), or with COR approval complete a vendor/platform specific certification (e.g., Microsoft Certified Solutions Developer (MCSD), Microsoft Certified Applications Developer (MCAD), Microsoft Certified Database Administrator (MCDBA), Red Hat Certification Program (RHCP), CISCO Certified Network Professional (CCNP), Oracle Certified Professional (OCP), other).
Experience: Six (6) years of in support of C5ISR systems/equipment, to include: Technology Analysis and Assessment, Design Definition, Development of Software Specifications, Systems Analysis, Systems and Software Architecture, Software Integration and Development, T&E Criteria, and Logistics support of C5ISR requirements. Note: Experience may be concurrent.

5. **Technical Analyst 1**

Education: BS degree in Physical Sciences, Mathematics, Psychology (NOTE: acceptable only if degree included courses in "Human Systems Interface (HSI)" and "Human Factors Engineering (HFE)").
Experience: One (1) year of experience in technical specifications development, process analysis and design, technical problem solving, and analytical/logical thinking.

6. **Operations Specialist**

Education: Bachelor's degree.
Experience: Ten (10) years of operational experience, to include: knowledge of friendly forces and adversary's CONOPS, tactics, threat capabilities, targeting priorities, sensor/collection techniques, targeting priorities, and planning and conducting operations analysis.

7. **Training Specialist 4**

Education: Bachelor's degree in Education, English, Psychology or Instructional Technology/Design, or related field. Training Certification.
Experience: Fifteen (15) years of experience in support of intelligence programs and systems, to include: establishing training needs, developing goals and objectives, developing training programs, and applying the instructional system development (ISD) process.

Service Contract Labor Standards – Wage Determination Categories

8. Computer Programmer II (14072)

Education: High School diploma or GED. Working towards completing the following certifications: Professional Software Engineering Master Certification (Previously known as Certified Software Development Professional (CSDP)), or with COR approval complete a vendor/platform specific certification (e.g., Microsoft Certified Solutions Developer (MCSD) Web Application or Application Lifecycle Management tracks, Microsoft Certified Solutions Expert (MCSE) Database or Server tracks, Oracle Certified Professional Java, CISCO Certified Network Professional (CCNP), other).
Experience: Three (3) years' experience, to include: software Design, and Development. One (1) year programming experience with PL/SQL, Java, C++ or C# programming languages.

9. Computer System Analyst II (14102)

Education: High School diploma or GED. Completed the following certifications within one and a half year after assuming duties: : Professional Software Engineering Master Certification (Previously known as Certified Software Development Professional (CSDP)), or with COR approval complete a vendor/platform specific certification (e.g., Microsoft Certified Solutions Developer (MCSD) Web Application or Application Lifecycle Management tracks, Microsoft Certified Solutions Expert (MCSE) Database or Server tracks, Oracle Certified Professional Java, CISCO Certified Network Professional (CCNP), Juniper Network Certified Internet Professional Enterprise Routing & Switching track, other).
Experience: Three (3) years of Computerized System experience, to include: Test and Evaluation, Network Protocols, LAN administration fundamentals, and UNIX and Windows based operating systems.

10. Computer System Analyst III (14103)

Education: High School diploma or GED. Completed the following certifications within one and a half year after assuming duties: Certified Software Development Professional (CSDP) (Previously known as Certified Software Engineering Professional (CSEP)), or with COR approval complete a vendor/platform specific certification (e.g., Microsoft Certified Solutions Developer (MCSD), Microsoft Certified Applications Developer (MCAD), Microsoft Certified Database Administrator (MCDBA), Sun Certified Professional (SCP), Red Hat Certification Program (RHCP), CISCO Certified Network Professional (CCNP), Oracle Certified Professional (OCP), other).
Experience: Five (5) years of Computerized System experience, to include: Design, Development, Test and Evaluation, Network Protocols, LAN administration fundamentals, and UNIX and Windows based operating systems.

(End of clause)

5252.237-9601 KEY PERSONNEL (DEC 1999)

(a) The offeror agrees to assign to this contract those key personnel listed in paragraph (d) below. No substitutions shall be made except in accordance with this clause.

(b) Offerors shall identify by name the proposed Program Manager as part of their proposal. After contract award, resumes for all individuals designated in key labor categories below shall be submitted and approved by the Government prior to performing tasking under this contract. The Government will review resumes of contractor personnel proposed to be assigned, and if personnel are not currently in the employ of Contractor, a written agreement to work from potential employees will be submitted to the Government.

The offeror agrees that during the first 90 days of the contract performance period no personnel substitutions will be permitted unless such substitutions are necessitated by an individual's sudden illness, death or termination of employment. In any of these events, the contractor shall promptly notify the Contracting Officer and provide the information required by paragraph (c) below. After the initial 90 day period, all proposed substitutions must be submitted in writing, at least fifteen (15) days (thirty (30) days if a security clearance is to be obtained) in advance of the proposed substitutions to the contracting officer. These substitution requests shall provide the information required by paragraph (c) below.

(c) All requests for approval of substitutions under this contract must be in writing and provide a detailed explanation of the circumstances necessitating the proposed substitutions. They must contain a complete resume for the proposed substitute or addition, and any other information requested by the Contracting Officer or needed by him to approve or disapprove the proposed substitutions. All substitutions proposed during the duration of this contract must have qualifications of the person being replaced. The Contracting Officer or his authorized representative will evaluate such requests and promptly notify the contractor of his approval or disapproval thereof in writing.

(d) List of Key Personnel

NAME	CONTRACT LABOR CATEGORY
*	Program Manager
**	Engineer/Scientist 5
**	Engineer/Scientist 4

* Program Manager shall be identified in the contract proposal.
** Other key personnel will be identified at task order level, when applicable.

(e) If the Contracting Officer determines that suitable and timely replacement of key personnel who have been reassigned, terminated or have otherwise become unavailable for the contract work is not reasonably forthcoming or that the resultant reduction of productive effort would be so substantial as to impair the successful completion of the contract or the service order, the contract may be terminated by the Contracting Officer for default or for the convenience of the Government, as appropriate. In addition, if the Contractor is found at fault for the condition, the Contracting Officer may elect to equitably decrease the contract price to compensate the Government for any resultant delay, loss or damage. Inability to manage, provide, and/or maintain sufficient key personnel shall negatively impact a contractor’s annual government Contractor Performance Assessment Report (CPAR) rating.

(f) If the offeror wishes to add personnel to be used in a labor category he shall employ the procedures outlined in paragraph (c) above. Adding personnel will only be permitted in the event of an indefinite quantity contract, where the Government has issued a delivery order for labor hours that would exceed a normal forty hour week if performed only by the number of employees originally proposed.

(End of clause)

INSPECTION AND ACCEPTANCE TERMS

Supplies/services will be inspected/accepted at:

CLIN	INSPECT AT	INSPECT BY	ACCEPT AT	ACCEPT BY
0001	Destination	Government	Destination	Government
0002	Destination	Government	Destination	Government
0003	Destination	Government	Destination	Government
0004	Destination	Government	Destination	Government
0005	Destination	Government	Destination	Government
0006	Destination	Government	Destination	Government
0007	Destination	Government	Destination	Government
0008	Destination	Government	Destination	Government
0009	Destination	Government	Destination	Government
0010	Destination	Government	Destination	Government
0011	Destination	Government	Destination	Government
0012	Destination	Government	Destination	Government

CLAUSES INCORPORATED BY REFERENCE

52.246-2	Inspection Of Supplies--Fixed Price	AUG 1996
52.246-4	Inspection Of Services--Fixed Price	AUG 1996
52.246-16	Responsibility For Supplies	APR 1984

Section F - Deliveries or Performance

DELIVERY INFORMATION

CLIN	DESCRIPTION	DELIVERY DATE	QUANTITY	SHIP TO ADDRESS
0001	Delivery of AATS Software - FFP	90 dys. ADC	1	FOB: Destination
0002	Delivery of AATS Software Documentation/ Technical Data Package – FFP	90 dys. ADC	1	FOB: Destination
0003	Delivery of AATS Systems Approach Training (SAT) Materials – FFP	180 dys. ADC	1	FOB: Destination
0005	Susatainment for AATS Software Delivered Under CLIN 0001 – Increment 1 - FFP	1 dy After Receipt of Order (ARO	1	FOB: Destination
0006	Susatainment for AATS Software Delivered Under CLIN 0001 – Increment 2 - FFP	1 dy ARO	1	FOB: Destination
0007	Susatainment for AATS Software Delivered Under CLIN 0001 – Increment 3 - FFP	1 dy ARO	1	FOB: Destination
0008	Susatainment for AATS Software Delivered Under CLIN 0001 – Increment 4 - FFP	1 dy ARO	1	FOB: Destination
0011	Contract Years 2 through 5 – Additional AATS Software Licenses/User Capacity - FFP	1 dy ARO	14	FOB: Destination

PERIODS OF PERFORMANCE

The period of performance of the contract, for the purpose of issuing task orders is as follows:

CLIN	DESCRIPTION	PERIOD OF PERFORMANCE FOR ISSUING ORDERS
0004	Original Equipment Manufacturer (OEM)/Subject Matter Expert (SME) Support for AATS Integration, Configuration, System Administration, Test, and IA	Date of contract award through sixty months thereafter
0009	AATS Pre-Planned Product Improvements	Start of contract year two through Forty-eight months thereafter
0010	Contract Data Requirements List (CDRL)	Date of contract award through sixty months thereafter
0012	Travel and Other Direct Costs	Date of contract award through sixty months thereafter

CLAUSES INCORPORATED BY REFERENCE

52.242-15	Stop-Work Order	AUG 1989
52.242-15 Alt I	Stop-Work Order (Aug 1989) - Alternate I	APR 1984
52.242-17	Government Delay Of Work	APR 1984
52.247-34	F.O.B. Destination	NOV 1991

Section G - Contract Administration Data

CLAUSES INCORPORATED BY FULL TEXT

252.204-7006 BILLING INSTRUCTIONS (OCT 2005)

When submitting a request for payment, the Contractor shall--

(a) Identify the contract line item(s) on the payment request that reasonably reflect contract work performance; and

(b) Separately identify a payment amount for each contract line item included in the payment request.

(End of clause)

252.232-7006 WIDE AREA WORKFLOW PAYMENT INSTRUCTIONS (MAY 2013)

(a) Definitions. As used in this clause--

Department of Defense Activity Address Code (DoDAAC) is a six position code that uniquely identifies a unit, activity, or organization.

Document type means the type of payment request or receiving report available for creation in Wide Area WorkFlow (WAWF).

Local processing office (LPO) is the office responsible for payment certification when payment certification is done external to the entitlement system.

(b) Electronic invoicing. The WAWF system is the method to electronically process vendor payment requests and receiving reports, as authorized by DFARS 252.232-7003, Electronic Submission of Payment Requests and Receiving Reports.

(c) WAWF access. To access WAWF, the Contractor shall--

(1) Have a designated electronic business point of contact in the System for Award Management at https://www.acquisition.gov; and

(2) Be registered to use WAWF at https://wawf.eb.mil/ following the step-by-step procedures for self-registration available at this Web site.

(d) WAWF training. The Contractor should follow the training instructions of the WAWF Web-Based Training Course and use the Practice Training Site before submitting payment requests through WAWF. Both can be accessed by selecting the “Web Based Training” link on the WAWF home page at https://wawf.eb.mil/.

(e) WAWF methods of document submission. Document submissions may be via Web entry, Electronic Data Interchange, or File Transfer Protocol.

(f) WAWF payment instructions. The Contractor must use the following information when submitting payment requests and receiving reports in WAWF for this contract/order:

(1) Document type. The Contractor shall use the following document type(s).

Fixed Price Orders - 2-N-1 (Services Only)

Note: If a “Combo” document type is identified but not supportable by the Contractor's business systems, an “Invoice” (stand-alone) and “Receiving Report” (stand-alone) document type may be used instead.

(2) Inspection/acceptance location. The Contractor shall select the following inspection/acceptance location(s) in WAWF, as specified by the contracting officer.

N65236

(3) Document routing. The Contractor shall use the information in the Routing Data Table below only to fill in applicable fields in WAWF when creating payment requests and receiving reports in the system.

Routing Data Table

Field Name in WAWF	*Data to be entered in WAWF*
	Fixed Price Orders
Pay Official DoDAAC	HQ0338
Issue By DoDAAC	N65236
Admin DoDAAC	S2404A
Inspect By DoDAAC	N65236
Ship To Code	N65236
Ship From Code	Not Applicable
Mark For Code	Not Applicable
Service Approver (DoDAAC)	N65236
Service Acceptor (DoDAAC)	N65236
Accept at Other DoDAAC	Not Applicable
LPO DoDAAC	Not Applicable
DCAA Auditor DoDAAC	Not Applicable
Other DoDAAC(s)	Not Applicable

(4) Payment request and supporting documentation. The Contractor shall ensure a payment request includes appropriate contract line item and subline item descriptions of the work performed or supplies delivered, unit price/cost per unit, fee (if applicable), and all relevant back-up documentation, as defined in DFARS Appendix F, (e.g. timesheets) in support of each payment request.

(5) WAWF email notifications. The Contractor shall enter the email address identified below in the “Send Additional Email Notifications” field of WAWF once a document is submitted in the system.

Not applicable

(g) WAWF point of contact. (1) The Contractor may obtain clarification regarding invoicing in WAWF from the following contracting activity's WAWF point of contact.

Not applicable

(2) For technical WAWF help, contact the WAWF helpdesk at 866-618-5988.

(End of clause)

5252.201-9201 DESIGNATION OF CONTRACTING OFFICER'S REPRESENTATIVE (MAR 2006)

(a) The Contracting Officer hereby appoints the following individual as Contracting Officer's Representative(s) (COR) for this contract/order:

CONTRACTING OFFICER REPRESENTATIVE

Name: *
Code: *
Address: *

Phone Number: *
E-mail: *

(b) It is emphasized that only the Contracting Officer has the authority to modify the terms of the contract, therefore, in no event will any understanding agreement, modification, change order, or other matter deviating from the terms of the basic contract between the Contractor and any other person be effective or binding on the Government. When/If, in the opinion of the Contractor, an effort outside the existing scope of the contract is requested, the Contractor shall promptly notify the PCO in writing. No action shall be taken by the Contractor unless the Procuring Contracting Officer (PCO) or the Administrative Contracting Officer (ACO) has issued a contractual change.

*To be assigned in individual task orders.

(End of clause)

5252.216-9210 TYPE OF CONTRACT (DEC 1999)

This is a single award, indefinite delivery/indefinite quantity type contract.

(End of clause)

Section H - Special Contract Requirements

CLAUSES INCORPORATED BY FULL TEXT

5252.204-9202 CONTRACTOR PICTURE BADGE (JUL 2013)

(a) A contractor picture badge may be issued to contractor personnel by the SPAWARSYSCEN Atlantic Security Office upon receipt of a valid visit request from the Contractor and a picture badge request from the COR. A list of personnel requiring picture badges must be provided to the COR to verify that the contract or delivery/task order authorizes performance at SPAWARSYSCEN Atlantic prior to completion of the picture badge request.

(b) The contractor assumes full responsibility for the proper use of the identification badge and shall be responsible for the return of the badge upon termination of personnel or expiration or completion of the contract.

(c) At the completion of the contract, the contractor shall forward to SPAWARSYSCEN Atlantic Security Office a list of all unreturned badges with a written explanation of any missing badges.

(End of clause)

5252.209-9206 EMPLOYMENT OF NAVY PERSONNEL RESTRICTED (DEC 1999)

In performing this contract, the Contractor will not use as a consultant or employ (on either a full or part-time basis) any active duty Navy personnel (civilian or military) without the prior approval of the Contracting Officer. Such approval may be given only in circumstances where it is clear that no law and no DOD or Navy instructions, regulations, or policies might possibly be contravened and no appearance of a conflict of interest will result.

(End of clause)

5252.216-9213 TYPES OF TASK OR DELIVERY ORDERS (DEC 1999)

The following types of task or delivery orders may be issued under this contract:

(a) A firm-fixed-price (FFP) delivery order will be issued when acquiring supplies on the basis of reasonably definite or detailed specifications and fair and reasonable prices can be established at the outset.

(b) A firm-fixed-price, level-of-effort (FFP-LOE) task order will be issued when acquiring services. The scope of work may define a definite goal or target which leads to an end product deliverable (e.g., a final report of research accomplishing the goal or target), or the scope of work may be defined in general terms and require that the contractor devote a specified LOE for a stated time period.

(End of clause)

5252.237-9602 CONTRACTOR IDENTIFICATION (MAY 2004)

(a) Contractor employees must be clearly identifiable while on Government property by wearing appropriate badges.

(b) Contractor personnel and their subcontractors must identify themselves as contractors or subcontractors during meetings, telephone conversations, in electronic messages, or correspondence related to this contract.

(c) Contractor-occupied facilities (on Department of the Navy or other Government installations) such as offices, separate rooms, or cubicles must be clearly identified with Contractor supplied signs, name plates or other identification, showing that these are work areas for Contractor or subcontractor personnel.

(End of clause)

5252.237-9603 REQUIRED INFORMATION ASSURANCE AND PERSONNEL SECURITY REQUIREMENTS FOR ACCESSING GOVERNMENT INFORMATION SYSTEMS AND NONPUBLIC INFORMATION (AUG 2011)

(a) Definition. As used in this clause, "sensitive information" includes:
- (i) All types and forms of confidential business information, including financial information relating to a contractor's pricing, rates, or costs, and program information relating to current or estimated budgets or schedules;
- (ii) Source selection information, including bid and proposal information as defined in FAR 2.101 and FAR 3.104-4, and other information prohibited from disclosure by the Procurement Integrity Act (41 USC 423);
- (iii) Information properly marked as "business confidential," "proprietary," "procurement sensitive," "source selection sensitive," or other similar markings;
- (iv) Other information designated as sensitive by the Space and Naval Warfare Systems Command (SPAWAR).

(b) In the performance of the contract, the Contractor may receive or have access to information, including information in Government Information Systems and secure websites. Accessed information may include "sensitive information" or other information not previously made available to the public that would be competitively useful on current or future related procurements.
(c) Contractors are obligated to protect and safeguard from unauthorized disclosure all sensitive information to which they receive access in the performance of the contract, whether the information comes from the Government or from third parties. The Contractor shall—
- (i) Utilize accessed information and limit access to authorized users only for the purposes of performing the services as required by the contract, and not for any other purpose unless authorized;
- (ii) Safeguard accessed information from unauthorized use and disclosure, and not discuss, divulge, or disclose any accessed information to any person or entity except those persons authorized to receive the information as required by the contract or as authorized by Federal statute, law, or regulation;
- (iii) Inform authorized users requiring access in the performance of the contract regarding their obligation to utilize information only for the purposes specified in the contact and to safeguard information from unauthorized use and disclosure.
- (iv) Execute a "Contractor Access to Information Non-Disclosure Agreement," and obtain and submit to the Contracting Officer a signed "Contractor Employee Access to Information Non-Disclosure Agreement" for each employee prior to assignment;
- (v) Notify the Contracting Officer in writing of any violation of the requirements in (i) through (iv) above as soon as the violation is identified, no later than 24 hours. The notice shall include a description of the violation and the proposed actions to be taken, and shall include the business organization, other entity, or individual to whom the information was divulged.

(d) In the event that the Contractor inadvertently accesses or receives any information marked as "proprietary," "procurement sensitive," or "source selection sensitive," or that, even if not properly marked otherwise indicates the Contractor may not be authorized to access such information, the Contractor shall (i) Notify the Contracting Officer; and (ii) Refrain from any further access until authorized in writing by the Contracting Officer.

(e) The requirements of this clause are in addition to any existing or subsequent Organizational Conflicts of Interest (OCI) requirements which may also be included in the contract, and are in addition to any personnel security or Information Assurance requirements, including Systems Authorization Access Request (SAAR-N), DD Form 2875, Annual Information Assurance (IA) training certificate, SF85P, or other forms that may be required for access to Government Information Systems.

(f) Subcontracts. The Contractor shall insert paragraphs (a) through (f) of this clause in all subcontracts that may require access to sensitive information in the performance of the contract.

(g) Mitigation Plan. If requested by the Contracting Officer, the contractor shall submit, within 45 calendar days following execution of the "Contractor Non-Disclosure Agreement," a mitigation plan for Government approval, which shall be incorporated into the contract. At a minimum, the mitigation plan shall identify the Contractor's plan to implement the requirements of paragraph (c) above and shall include the use of a firewall to separate Contractor personnel requiring access to information in the performance of the contract from other Contractor personnel to ensure that the Contractor does not obtain any unfair competitive advantage with respect to any future Government requirements due to unequal access to information. A "firewall" may consist of organizational and physical separation; facility and workspace access restrictions; information system access restrictions; and other data security measures identified, as appropriate. The Contractor shall respond promptly to all inquiries regarding the mitigation plan. Failure to resolve any outstanding issues or obtain approval of the mitigation plan within 45 calendar days of its submission may result, at a minimum, in rejection of the plan and removal of any system access.

(End of clause)

5252.227-9207 ALT I

LIMITED RELEASE OF CONTRACTOR CONFIDENTIAL BUSINESS INFORMATION (APRIL 2010) ALTERNATE I (JAN 2012)

(a) Definition.
"Confidential Business Information," (Information) as used in this clause, is defined as all forms and types of financial, business, economic or other types of information including technical data or computer software/computer software documentation, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing even when -- (1) the owner thereof has taken reasonable measures to keep such information secret, and (2) the Information derives independent economic value, actual or potential from not being generally known to, and not being readily ascertainable through proper means by, the public. Information will include technical data, as that term is defined in DFARS 252.227-7013(a)(14), 252.227-7015(a)(4), and 252.227-7018(a)(19). Similarly, Information does include computer software/computer software documentation, as those terms are defined in DFARS 252.227-7014(a)(4) and 252.227-7018(a)(4).

(b) The Space and Naval Warfare Systems Command (SPAWAR) may release to individuals employed by SPAWAR support contractors and their subcontractors Information submitted by the contractor or its subcontractors pursuant to the provisions of this contract. Information that would ordinarily be entitled to confidential treatment may be included in the Information released to these individuals. Accordingly, by submission of a proposal or execution of this contract, the offeror or contractor and its subcontractors consent to a limited release of its Information, but only for purposes as described in paragraph (c) of this clause.

(c) Circumstances where SPAWAR may release the contractor's or subcontractors' Information include the following:

(1) To other SPAWAR contractors and subcontractors, and their employees tasked with assisting SPAWAR in handling and processing Information and documents in the administration of SPAWAR contracts, such as file room management and contract closeout; and,
(2) To SPAWAR contractors and subcontractors, and their employees tasked with assisting SPAWAR in accounting support services, including access to cost-reimbursement vouchers.

(d) SPAWAR recognizes its obligation to protect the contractor and its subcontractors from competitive harm that could result from the release of such Information. SPAWAR will permit the limited release of Information under paragraphs (c)(1), (c)(2), (c)(3), and (c)(4) only under the following conditions:
(1) SPAWAR determines that access is required by other SPAWAR contractors and their subcontractors to perform the tasks described in paragraphs (c)(1), (c)(2), (c)(3), and (c)(4);
(2) Access to Information is restricted to individuals with a bona fide need to possess;
(3) Contractors and their subcontractors having access to Information have agreed under their contract or a separate corporate non-disclosure agreement to provide the same level of protection to the Information that would be provided by SPAWAR employees. Such contract terms or separate corporate non-disclosure agreement shall require the contractors and subcontractors to train their employees on how to properly handle the Information to which they will have access, and to have their employees sign company non disclosure agreements certifying that they understand the sensitive nature of the Information and that unauthorized use of the Information could expose their company to significant liability. Copies of such employee non disclosure agreements shall be provided to the Government;
(4) SPAWAR contractors and their subcontractors performing the tasks described in paragraphs (c)(1), (c)(2), (c)(3), and (c)(4) have agreed under their contract or a separate non-disclosure agreement to not use the Information for any purpose other than performing the tasks described in paragraphs (c)(1), (c)(2), (c)(3), and (c)(4); and,
(5) Before releasing the Information to a non-Government person to perform the tasks described in paragraphs (c)(1), (c)(2), (c)(3), and (c)(4), SPAWAR shall provide the contractor a list of the company names to which access is being granted, along with a Point of Contact for those entities.

(e) SPAWAR's responsibilities under the Freedom of Information Act are not affected by this clause.

(f) The contractor agrees to include, and require inclusion of, this clause in all subcontracts at any tier that requires the furnishing of Information.

(End of Clause)

Section I - Contract Clauses

CLAUSES INCORPORATED BY REFERENCE

52.202-1	Definitions	NOV 2013
52.203-3	Gratuities	APR 1984
52.203-5	Covenant Against Contingent Fees	MAY 2014
52.203-6	Restrictions On Subcontractor Sales To The Government	SEP 2006
52.203-7	Anti-Kickback Procedures	MAY 2014
52.203-8	Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity	MAY 2014
52.203-10	Price Or Fee Adjustment For Illegal Or Improper Activity	MAY 2014
52.203-12	Limitation On Payments To Influence Certain Federal Transactions	OCT 2010
52.203-13	Contractor Code of Business Ethics and Conduct	OCT 2015
52.203-16	Preventing Personal Conflicts of Interest	DEC 2011
52.203-17	Contractor Employee Whistleblower Rights and Requirement To Inform Employees of Whistleblower Rights	APR 2014
52.204-2	Security Requirements	AUG 1996
52.204-4	Printed or Copied Double-Sided on Postconsumer Fiber Content Paper	MAY 2011
52.204-9	Personal Identity Verification of Contractor Personnel	JAN 2011
52.204-10	Reporting Executive Compensation and First-Tier Subcontract Awards	OCT 2016
52.204-13	System for Award Management Maintenance	OCT 2016
52.204-22	Alternative Line Item Proposal	JAN 2017
52.209-6	Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment	OCT 2015
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters	JUL 2013
52.209-10	Prohibition on Contracting With Inverted Domestic Corporations	NOV 2015
52.210-1	Market Research	APR 2011
52.211-5	Material Requirements	AUG 2000
52.211-15	Defense Priority And Allocation Requirements	APR 2008
52.215-2	Audit and Records--Negotiation	OCT 2010
52.215-8	Order of Precedence--Uniform Contract Format	OCT 1997
52.215-11	Price Reduction for Defective Certified Cost or Pricing Data--Modifications	AUG 2011
52.215-13	Subcontractor Certified Cost or Pricing Data--Modifications	OCT 2010
52.215-14	Integrity of Unit Prices	OCT 2010
52.215-17	Waiver of Facilities Capital Cost of Money	OCT 1997
52.215-18	Reversion or Adjustment of Plans for Postretirement Benefits (PRB) Other than Pensions	JUL 2005
52.215-19	Notification of Ownership Changes	OCT 1997
52.215-21	Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data -- Modifications	OCT 2010
52.215-21 Alt III	Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data -- Modifications (Oct 2010) - Alternate III	OCT 1997
52.215-23 Alt I	Limitations on Pass-Through Charges (Oct 2009) - Alternate I	OCT 2009
52.217-6	Option For Increased Quantity	MAR 1989

52.219-4	Notice of Price Evaluation Preference for HUBZone Small Business Concerns	OCT 2014
52.219-8	Utilization of Small Business Concerns	NOV 2016
52.219-9	Small Business Subcontracting Plan	JAN 2017
52.219-9 Alt II	Small Business Subcontracting Plan (JAN 2017) Alternate II	NOV 2016
52.219-16	Liquidated Damages-Subcontracting Plan	JAN 1999
52.219-28	Post-Award Small Business Program Rerepresentation	JUL 2013
52.222-3	Convict Labor	JUN 2003
52.222-19	Child Labor -- Cooperation with Authorities and Remedies	OCT 2016
52.222-21	Prohibition Of Segregated Facilities	APR 2015
52.222-26	Equal Opportunity	SEP 2016
52.222-29	Notification Of Visa Denial	APR 2015
52.222-35	Equal Opportunity for Veterans	OCT 2015
52.222-36	Equal Opportunity for Workers with Disabilities	JUL 2014
52.222-37	Employment Reports on Veterans	FEB 2016
52.222-40	Notification of Employee Rights Under the National Labor Relations Act	DEC 2010
52.222-41	Service Contract Labor Standards	MAY 2014
52.222-43	Fair Labor Standards Act And Service Contract Labor Standards - Price Adjustment (Multiple Year And Option Contracts)	MAY 2014
52.222-50	Combating Trafficking in Persons	MAR 2015
52.222-54	Employment Eligibility Verification	OCT 2015
52.222-55	Minimum Wages Under Executive Order 13658	DEC 2015
52.223-5	Pollution Prevention and Right-to-Know Information	MAY 2011
52.223-6	Drug-Free Workplace	MAY 2001
52.223-10	Waste Reduction Program	MAY 2011
52.223-18	Encouraging Contractor Policies To Ban Text Messaging While Driving	AUG 2011
52.224-1	Privacy Act Notification	APR 1984
52.224-2	Privacy Act	APR 1984
52.225-1	Buy American--Supplies	MAY 2014
52.225-19	Contractor Personnel in a Designated Operational Area or Supporting a Diplomatic or Consular Mission Outside the United States	MAR 2008
52.227-1	Authorization and Consent	DEC 2007
52.227-2	Notice And Assistance Regarding Patent And Copyright Infringement	DEC 2007
52.227-3	Patent Indemnity	APR 1984
52.227-3 Alt I	Patent Indemnity (Apr 1984) - Alternate I	APR 1984
52.228-7	Insurance--Liability To Third Persons	MAR 1996
52.229-3	Federal, State And Local Taxes	FEB 2013
52.232-1	Payments	APR 1984
52.232-8	Discounts For Prompt Payment	FEB 2002
52.232-11	Extras	APR 1984
52.232-17	Interest	MAY 2014
52.232-18	Availability Of Funds	APR 1984
52.232-23	Assignment Of Claims	MAY 2014
52.232-25	Prompt Payment	JAN 2017
52.232-25 Alt I	Prompt Payment (Jan 2017) Alternate I	FEB 2002
52.232-33	Payment by Electronic Funds Transfer--System for Award Management	JUL 2013
52.232-39	Unenforceability of Unauthorized Obligations	JUN 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	DEC 2013

52.233-1	Disputes	MAY 2014
52.233-1 Alt I	Disputes (May 2014) - Alternate I	DEC 1991
52.233-3	Protest After Award	AUG 1996
52.233-3 Alt I	Protest After Award (Aug 1996) - Alternate I	JUN 1985
52.233-4	Applicable Law for Breach of Contract Claim	OCT 2004
52.237-2	Protection Of Government Buildings, Equipment, And Vegetation	APR 1984
52.237-3	Continuity Of Services	JAN 1991
52.239-1	Privacy or Security Safeguards	AUG 1996
52.242-3	Penalties for Unallowable Costs	MAY 2014
52.242-4	Certification of Final Indirect Costs	JAN 1997
52.242-13	Bankruptcy	JUL 1995
52.243-1	Changes--Fixed Price	AUG 1987
52.244-5	Competition In Subcontracting	DEC 1996
52.244-6	Subcontracts for Commercial Items	JAN 2017
52.247-63	Preference For U.S. Flag Air Carriers	JUN 2003
52.247-64	Preference for Privately Owned U.S. - Flag Commercial Vessels	FEB 2006
52.248-1	Value Engineering	OCT 2010
52.249-2	Termination For Convenience Of The Government (Fixed-Price)	APR 2012
52.249-8	Default (Fixed-Price Supply & Service)	APR 1984
52.249-14	Excusable Delays	APR 1984
52.251-1	Government Supply Sources	APR 2012
52.253-1	Computer Generated Forms	JAN 1991
252.201-7000	Contracting Officer's Representative	DEC 1991
252.203-7000	Requirements Relating to Compensation of Former DoD Officials	SEP 2011
252.203-7001	Prohibition On Persons Convicted of Fraud or Other Defense-Contract-Related Felonies	DEC 2008
252.203-7002	Requirement to Inform Employees of Whistleblower Rights	SEP 2013
252.203-7003	Agency Office of the Inspector General	DEC 2012
252.203-7004	Display of Hotline Posters	OCT 2016
252.204-7000	Disclosure Of Information	OCT 2016
252.204-7002	Payment For Subline Items Not Separately Priced	DEC 1991
252.204-7003	Control Of Government Personnel Work Product	APR 1992
252.204-7005	Oral Attestation of Security Responsibilities	NOV 2001
252.204-7009	Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information	OCT 2016
252.204-7014	Limitations on the Use or Disclosure of Information by Litigation Support Contractors	MAY 2016
252.205-7000	Provision Of Information To Cooperative Agreement Holders	DEC 1991
252.209-7004	Subcontracting With Firms That Are Owned or Controlled By The Government of a Country that is a State Sponsor of Terrorism	OCT 2015
252.211-7003	Item Unique Identification and Valuation	MAR 2016
252.211-7005	Substitutions for Military or Federal Specifications and Standards	NOV 2005
252.211-7008	Use of Government-Assigned Serial Numbers	SEP 2010
252.215-7000	Pricing Adjustments	DEC 2012
252.219-7003	Small Business Subcontracting Plan (DOD Contracts)--Basic	MAR 2016
252.219-7003 (Dev)	Small Business Subcontracting Plan (DOD Contracts)--Basic (Deviation 2016-O0009)	AUG 2016
252.222-7002	Compliance With Local Labor Laws (Overseas)	JUN 1997
252.223-7004	Drug Free Work Force	SEP 1988

252.223-7006	Prohibition On Storage, Treatment, and Disposal of Toxic or Hazardous Materials	SEP 2014
252.223-7008	Prohibition of Hexavalent Chromium	JUN 2013
252.225-7001	Buy American And Balance Of Payments Program-- Basic (Dec 2016)	DEC 2016
252.225-7002	Qualifying Country Sources As Subcontractors	DEC 2016
252.225-7004	Report of Intended Performance Outside the United States and Canada--Submission after Award	OCT 2015
252.225-7012	Preference For Certain Domestic Commodities	DEC 2016
252.225-7013	Duty-Free Entry--Basic (May 2016)	MAY 2016
252.225-7021	Trade Agreements--Basic	DEC 2016
252.225-7041	Correspondence in English	JUN 1997
252.225-7043	Antiterrorism/Force Protection Policy for Defense Contractors Outside the United States	JUN 2015
252.225-7048	Export-Controlled Items	JUN 2013
252.225-7995 (Dev)	Contractor Personnel Performing in the United States Central Command Area of Responsibility (Deviation)	JAN 2015
252.226-7001	Utilization of Indian Organizations and Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns	SEP 2004
252.227-7013	Rights in Technical Data--Noncommercial Items	FEB 2014
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	FEB 2014
252.227-7015	Technical Data--Commercial Items	FEB 2014
252.227-7016	Rights in Bid or Proposal Information	JAN 2011
252.227-7019	Validation of Asserted Restrictions--Computer Software	SEP 2016
252.227-7025	Limitations on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends	MAY 2013
252.227-7026	Deferred Delivery Of Technical Data Or Computer Software	APR 1988
252.227-7027	Deferred Ordering Of Technical Data Or Computer Software	APR 1988
252.227-7030	Technical Data--Withholding Of Payment	MAR 2000
252.227-7037	Validation of Restrictive Markings on Technical Data	SEP 2016
252.232-7003	Electronic Submission of Payment Requests and Receiving Reports	JUN 2012
252.232-7010	Levies on Contract Payments	DEC 2006
252.237-7010	Prohibition on Interrogation of Detainees by Contractor Personnel	JUN 2013
252.239-7001	Information Assurance Contractor Training and Certification	JAN 2008
252.242-7004	Material Management And Accounting System	MAY 2011
252.242-7005	Contractor Business Systems	FEB 2012
252.242-7006	Accounting System Administration	FEB 2012
252.243-7001	Pricing Of Contract Modifications	DEC 1991
252.243-7002	Requests for Equitable Adjustment	DEC 2012
252.244-7000	Subcontracts for Commercial Items	JUN 2013
252.244-7001	Contractor Purchasing System Administration	MAY 2014
252.246-7000	Material Inspection And Receiving Report	MAR 2008

CLAUSES INCORPORATED BY FULL TEXT

52.216-19 ORDER LIMITATIONS. (OCT 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than $25,000, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those

supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor:

(1) Any order for a single item in excess of the total contract ceiling amount;

(2) Any order for a combination of items in excess of the total contract ceiling amount; or

(3) A series of orders from the same ordering office within the contract period of performance that together call for quantities exceeding the limitation in subparagraph (1) or (2) above.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) above.

(d) Notwithstanding paragraphs (b) and (c) above, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within seven days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of clause)

52.216-22 INDEFINITE QUANTITY. (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum". The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum".

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after twelve (12) months of contract expiration.

(End of clause)

52.222-42 STATEMENT OF EQUIVALENT RATES FOR FEDERAL HIRES (MAY 2014)

In compliance with the Service Contract Labor Standards statute and the regulations of the Secretary of Labor (29 CFR part 4), this clause identifies the classes of service employees expected to be employed under the contract and states the wages and fringe benefits payable to each if they were employed by the contracting agency subject to the provisions of 5 U.S.C. 5341 or 5332.

THIS STATEMENT IS FOR INFORMATION ONLY: IT IS NOT A WAGE DETERMINATION

Employee Class	SCLS #	Monetary Wage - Fringe Benefits
Computer Programmer II	(SCLS 14072)	GS-7
Computer Systems Analyst II	(SCLS 14102)	GS-11
Computer Systems Analyst III	(SCLS 14103)	GS-12

(End of clause)

52.225-13 RESTRICTIONS ON CERTAIN FOREIGN PURCHASES (JUN 2008)

(a) Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this contract, any supplies or services if any proclamation, Executive order, or statute administered by OFAC, or if OFAC's implementing regulations at 31 CFR chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.

(b) Except as authorized by OFAC, most transactions involving Cuba, Iran, and Sudan are prohibited, as are most imports from Burma or North Korea, into the United States or its outlying areas. Lists of entities and individuals subject to economic sanctions are included in OFAC's List of Specially Designated Nationals and Blocked Persons at TerList1.html. More information about these restrictions, as well as updates, is available in the OFAC's regulations at 31 CFR chapter V and/or on OFAC's Web site at http://www.treas.gov/offices/enforcement/ofac/.

(c) The Contractor shall insert this clause, including this paragraph (c), in all subcontracts.

(End of clause)

52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

http://farsite.hill.af.mil
http://www.acquisition.gov/far

(End of clause)

52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Defense Federal Acquisition Regulation Supplement (DFARS) (48 CFR Chapter 2) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of clause)

252.203-7004 DISPLAY OF HOTLINE POSTERS (OCT 2016)

(a) Definition. United States, as used in this clause, means the 50 States, the District of Columbia, and outlying areas.

(b) Display of hotline poster(s).

(1)(i) The Contractor shall display prominently the DoD fraud, waste, and abuse hotline poster prepared by the DoD Office of the Inspector General, in effect at time of contract award, in common work areas within business segments performing work under Department of Defense (DoD) contracts.

(ii) For contracts performed outside the United States, when security concerns can be appropriately demonstrated, the contracting officer may provide the contractor the option to publicize the program to contractor personnel in a manner other than public display of the poster, such as private employee written instructions and briefings.

(2) If the contract is funded, in whole or in part, by Department of Homeland Security (DHS) disaster relief funds and the work is to be performed in the United States, the DHS fraud hotline poster shall be displayed in addition to the DoD hotline poster. If a display of a DHS fraud hotline poster is required, the Contractor may obtain such poster from--

(i) DHS Office of Inspector General/MAIL STOP 0305, Attn: Office of Investigations--Hotline, 245 Murray Lane SW., Washington, DC 20528-0305; or

(ii) Via the Internet at https://www.oig.dhs.gov/assets/Hotline/DHS_OIG_Hotline-optimized.jpg.

(c)(1) The DoD hotline poster may be obtained from: Defense Hotline, The Pentagon, Washington, DC 20301-1900, or is also available via the internet at http://www.dodig.mil/hotline/hotline_posters.htm.

(2) If a significant portion of the employee workforce does not speak English, then the poster is to be displayed in the foreign languages that a significant portion of the employees speak.

(3) Additionally, if the Contractor maintains a company Web site as a method of providing information to employees, the Contractor shall display an electronic version of the required poster at the Web site.

(d) Subcontracts. The Contractor shall include this clause, including this paragraph (d), in all subcontracts that exceed $5.5 million except when the subcontract is for the acquisition of a commercial item.

(End of clause)

252.204-7012 SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016)

(a) Definitions. As used in this clause--

Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Compromise means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.

Controlled technical information means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

Covered contractor information system means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

Covered defense information means unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is--

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Malicious software means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

Media means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

Operationally critical support means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

Rapidly report means within 72 hours of discovery of any cyber incident.

Technical information means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data--Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) Adequate security. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:

(1) For covered contractor information systems that are part of an information technology (IT) service or system operated on behalf of the Government, the following security requirements apply:

(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.

(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:

(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, ``Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations'' (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.

(ii)(A) The Contractor shall implement NIST SP 800-171, as soon aspractical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2)

of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

(c) Cyber incident reporting requirement.

(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall--

(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and

(ii) Rapidly report cyber incidents to DoD at http://dibnet.dod.mil.

(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil.

(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx.

(d) Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

(e) Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

(f) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

(g) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

(h) DoD safeguarding and use of contractor attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.

(i) Use and release of contractor attributional/proprietary information not created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD--

(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;

(3) To Government entities that conduct counterintelligence or law enforcement investigations;

(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or

(5) To a support services contractor (``recipient'') that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.

(j) Use and release of contractor attributional/proprietary information created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.

(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.

(l) Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.

(m) Subcontracts. The Contractor shall--

(1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, for operationally critical support, or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and

(2) Require subcontractors to--

(i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and

(ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.

(End of clause)

252.211-7003 ITEM UNIQUE IDENTIFICATION AND VALUATION (MAR 2016)

(a) Definitions. As used in this clause-

Automatic identification device means a device, such as a reader or interrogator, used to retrieve data encoded on machine-readable media.

Concatenated unique item identifier means--

(1) For items that are serialized within the enterprise identifier, the linking together of the unique identifier data elements in order of the issuing agency code, enterprise identifier, and unique serial number within the enterprise identifier; or

(2) For items that are serialized within the original part, lot, or batch number, the linking together of the unique identifier data elements in order of the issuing agency code; enterprise identifier; original part, lot, or batch number; and serial number within the original part, lot, or batch number.

Data Matrix means a two-dimensional matrix symbology, which is made up of square or, in some cases, round modules arranged within a perimeter finder pattern and uses the Error Checking and Correction 200 (ECC200) specification found within International Standards Organization (ISO)/International Electrotechnical Commission (IEC) 16022.

Data qualifier means a specified character (or string of characters) that immediately precedes a data field that defines the general category or intended use of the data that follows.

DoD recognized unique identification equivalent means a unique identification method that is in commercial use and has been recognized by DoD. All DoD recognized unique identification equivalents are listed at http://www.acq.osd.mil/dpap/pdi/uid/iuid_equivalents.html.

DoD item unique identification means a system of marking items delivered to DoD with unique item identifiers that have machine-readable data elements to distinguish an item from all other like and unlike items. For items that are serialized within the enterprise identifier, the unique item identifier shall include the data elements of the enterprise identifier and a unique serial number. For items that are serialized within the part, lot, or batch number within the enterprise identifier, the unique item identifier shall include the data elements of the enterprise identifier; the original part, lot, or batch number; and the serial number.

Enterprise means the entity (e.g., a manufacturer or vendor) responsible for assigning unique item identifiers to items.

Enterprise identifier means a code that is uniquely assigned to an enterprise by an issuing agency.

Government's unit acquisition cost means--

(1) For fixed-price type line, subline, or exhibit line items, the unit price identified in the contract at the time of delivery;

(2) For cost-type or undefinitized line, subline, or exhibit line items, the Contractor's estimated fully burdened unit cost to the Government at the time of delivery; and

(3) For items produced under a time-and-materials contract, the Contractor's estimated fully burdened unit cost to the Government at the time of delivery.

Issuing agency means an organization responsible for assigning a globally unique identifier to an enterprise, as indicated in the Register of Issuing Agency Codes for ISO/IEC 15459, located at http://www.aimglobal.org/?Reg_Authority15459.

Issuing agency code means a code that designates the registration (or controlling) authority for the enterprise identifier.

Item means a single hardware article or a single unit formed by a grouping of subassemblies, components, or constituent parts.

Lot or batch number means an identifying number assigned by the enterprise to a designated group of items, usually referred to as either a lot or a batch, all of which were manufactured under identical conditions.

Machine-readable means an automatic identification technology media, such as bar codes, contact memory buttons, radio frequency identification, or optical memory cards.

Original part number means a combination of numbers or letters assigned by the enterprise at item creation to a class of items with the same form, fit, function, and interface.

Parent item means the item assembly, intermediate component, or subassembly that has an embedded item with a unique item identifier or DoD recognized unique identification equivalent.

Serial number within the enterprise identifier means a combination of numbers, letters, or symbols assigned by the enterprise to an item that provides for the differentiation of that item from any other like and unlike item and is never used again within the enterprise.

Serial number within the part, lot, or batch number means a combination of numbers or letters assigned by the enterprise to an item that provides for the differentiation of that item from any other like item within a part, lot, or batch number assignment.

Serialization within the enterprise identifier means each item produced is assigned a serial number that is unique among all the tangible items produced by the enterprise and is never used again. The enterprise is responsible for ensuring unique serialization within the enterprise identifier.

Serialization within the part, lot, or batch number means each item of a particular part, lot, or batch number is assigned a unique serial number within that part, lot, or batch number assignment. The enterprise is responsible for ensuring unique serialization within the part, lot, or batch number within the enterprise identifier.

Type designation means a combination of letters and numerals assigned by the Government to a major end item, assembly or subassembly, as appropriate, to provide a convenient means of differentiating between items having the same basic name and to indicate modifications and changes thereto.

Unique item identifier means a set of data elements marked on items that is globally unique and unambiguous. The term includes a concatenated unique item identifier or a DoD recognized unique identification equivalent.

Unique item identifier type means a designator to indicate which method of uniquely identifying a part has been used. The current list of accepted unique item identifier types is maintained at http://www.acq.osd.mil/dpap/pdi/uid/uii_types.html.

(b) The Contractor shall deliver all items under a contract line, subline, or exhibit line item.

(c) Unique item identifier. (1) The Contractor shall provide a unique item identifier for the following:

(i) Delivered items for which the Government's unit acquisition cost is $5,000 or more, except for the following line items:

Contract line, subline, or exhibit line item No.	Item description
.....	

(ii) Items for which the Government's unit acquisition cost is less than $5,000 that are identified in the Schedule or the following table:

Contract line, subline, or exhibit line item No.	Item description
.....	

(If items are identified in the Schedule, insert ``See Schedule'' in this table.)

(iii) Subassemblies, components, and parts embedded within delivered items, items with warranty requirements, DoD serially managed reparables and DoD serially managed nonreparables as specified in Attachment Number ----.

(iv) Any item of special tooling or special test equipment as defined in FAR 2.101 that have been designated for preservation and storage for a Major Defense Acquisition Program as specified in Attachment Number ----.

(v) Any item not included in paragraphs (c)(1)(i), (ii), (iii), or

(iv) of this clause for which the contractor creates and marks a unique item identifier for traceability.

(2) The unique item identifier assignment and its component data element combination shall not be duplicated on any other item marked or registered in the DoD Item Unique Identification Registry by the contractor.

(3) The unique item identifier component data elements shall be marked on an item using two dimensional data matrix symbology that complies with ISO/IEC International Standard 16022, Information technology--International symbology specification--Data matrix; ECC200 data matrix specification.

(4) Data syntax and semantics of unique item identifiers. The Contractor shall ensure that--

(i) The data elements (except issuing agency code) of the unique item identifier are encoded within the data matrix symbol that is marked on the item using one of the following three types of data qualifiers, as determined by the Contractor:

(A) Application Identifiers (AIs) (Format Indicator 05 of ISO/IEC International Standard 15434), in accordance with ISO/IEC International Standard 15418, Information Technology--EAN/UCC Application Identifiers and Fact Data Identifiers and Maintenance and ANSI MH 10.8.2 Data Identifier and Application Identifier Standard.

(B) Data Identifiers (DIs) (Format Indicator 06 of ISO/IEC International Standard 15434), in accordance with ISO/IEC International Standard 15418, Information Technology--EAN/UCC Application Identifiers and Fact Data Identifiers and Maintenance and ANSI MH 10.8.2 Data Identifier and Application Identifier Standard.

(C) Text Element Identifiers (TEIs) (Format Indicator 12 of ISO/IEC International Standard 15434), in accordance with the Air Transport Association Common Support Data Dictionary; and

(ii) The encoded data elements of the unique item identifier conform to the transfer structure, syntax, and coding of messages and data formats specified for Format Indicators 05, 06, and 12 in ISO/IEC International Standard 15434, Information Technology-Transfer Syntax for High Capacity Automatic Data Capture Media.

(5) Unique item identifier.

(i) The Contractor shall--

(A) Determine whether to--

(1) Serialize within the enterprise identifier;

(2) Serialize within the part, lot, or batch number; or

(3) Use a DoD recognized unique identification equivalent (e.g. Vehicle Identification Number); and

(B) Place the data elements of the unique item identifier (enterprise identifier; serial number; DoD recognized unique
identification equivalent; and for serialization within the part, lot, or batch number only: Original part, lot, or batch number) on items requiring marking by paragraph (c)(1) of this clause, based on the criteria provided in MIL-STD-130, Identification Marking of U.S. Military Property, latest version;

(C) Label shipments, storage containers and packages that contain uniquely identified items in accordance with the requirements of MIL-STD-129, Military Marking for Shipment and Storage, latest version; and

(D) Verify that the marks on items and labels on shipments, storage containers, and packages are machine readable and conform to the applicable standards. The contractor shall use an automatic identification technology device for this verification that has been programmed to the requirements of Appendix A, MIL-STD-130, latest version.

(ii) The issuing agency code--

(A) Shall not be placed on the item; and

(B) Shall be derived from the data qualifier for the enterprise identifier.

(d) For each item that requires item unique identification under paragraph (c)(1)(i), (ii), or (iv) of this clause or when item unique identification is provided under paragraph (c)(1)(v), in addition to the information provided as part of the Material Inspection and Receiving Report specified elsewhere in this contract, the Contractor shall report at the time of delivery, as part of the Material Inspection and Receiving Report, the following information:

(1) Unique item identifier.

(2) Unique item identifier type.

(3) Issuing agency code (if concatenated unique item identifier is used).

(4) Enterprise identifier (if concatenated unique item identifier is used).

(5) Original part number (if there is serialization within the original part number).

(6) Lot or batch number (if there is serialization within the lot or batch number).

(7) Current part number (optional and only if not the same as the original part number).

(8) Current part number effective date (optional and only if current part number is used).

(9) Serial number (if concatenated unique item identifier is used).

(10) Government's unit acquisition cost.

(11) Unit of measure.

(12) Type designation of the item as specified in the contract schedule, if any.

(13) Whether the item is an item of Special Tooling or Special Test Equipment.

(14) Whether the item is covered by a warranty.

(e) For embedded subassemblies, components, and parts that require DoD unique item identification under paragraph (c)(1)(iii) of this clause, the Contractor shall report as part of, or associated with, the Material Inspection and Receiving Report specified elsewhere in this contract, the following information:

(1) Unique item identifier of the parent item under paragraph (c)(1) of this clause that contains the embedded subassembly, component, or part.

(2) Unique item identifier of the embedded subassembly, component, or part.

(3) Unique item identifier type.**

(4) Issuing agency code (if concatenated unique item identifier is used).**

(5) Enterprise identifier (if concatenated unique item identifier is used).**

(6) Original part number (if there is serialization within the original part number).**

(7) Lot or batch number (if there is serialization within the lot or batch number).**

(8) Current part number (optional and only if not the same as the original part number).**

(9) Current part number effective date (optional and only if current part number is used).**

(10) Serial number (if concatenated unique item identifier is used).**

(11) Description.

** Once per item.

(f) The Contractor shall submit the information required by paragraphs (d) and (e) of this clause as follows:

(1) End items shall be reported using the receiving report capability in Wide Area WorkFlow (WAWF) in accordance with the clause at 252.232-7003. If WAWF is not required by this contract, and the contractor is not using WAWF, follow the procedures at http://dodprocurementtoolbox.com/site/uidregistry/.

(2) Embedded items shall be reported by one of the following methods--

(i) Use of the embedded items capability in WAWF;

(ii) Direct data submission to the IUID Registry following the procedures and formats at http://dodprocurementtoolbox.com/site/uidregistry/; or

(iii) Via WAWF as a deliverable attachment for exhibit line item number (fill in) ----, Unique Item Identifier Report for Embedded Items, Contract Data Requirements List, DD Form 1423.

(g) Subcontracts. If the Contractor acquires by subcontract any items for which item unique identification is required in accordance with paragraph (c)(1) of this clause, the Contractor shall include this clause, including this paragraph (g), in the applicable subcontract(s), including subcontracts for commercial items.

(End of clause)

252.216-7006 ORDERING (MAY 2011)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the contract schedule. Such orders may be issued from contract through five years thereafter.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c)(1) If issued electronically, the order is considered ``issued'' when a copy has been posted to the Electronic Document Access system, and notice has been sent to the Contractor.

(2) If mailed or transmitted by facsimile, a delivery order or task order is considered ``issued'' when the Government deposits the order in the mail or transmits by facsimile. Mailing includes transmittal by U.S. mail or private delivery services.

(3) Orders may be issued orally only if authorized in the
schedule.

(End of Clause)

252.222-7000 RESTRICTIONS ON EMPLOYMENT OF PERSONNEL (MAR 2000)

(a) The Contractor shall employ, for the purpose of performing that portion of the contract work in ___*___, individuals who are residents thereof and who, in the case of any craft or trade, possess or would be able to acquire promptly the necessary skills to perform the contract.

(b) The Contractor shall insert the substance of this clause, including this paragraph (b), in each subcontract awarded under this contract.

*To be completed on individual task orders.

(End of clause)

252.246-7006 Warranty Tracking of Serialized Items (MAR 2016)

(a) Definitions. As used in this clause--

Duration means the warranty period. This period may be a stated period of time, amount of usage, or the occurrence of a specified event, after formal acceptance of delivery, for the Government to assert a contractual right for the correction of defects.

Enterprise means the entity (e.g., a manufacturer or vendor) responsible for granting the warranty and/or assigning unique item identifiers to serialized warranty items.

Enterprise identifier means a code that is uniquely assigned to an enterprise by an issuing agency.

First use means the initial or first-time use of a product by the Government.

Fixed expiration means the date the warranty expires and the Contractor's obligation to provide for a remedy or corrective action ends.

Installation means the date a unit is inserted into a higher level assembly in order to make that assembly operational.

Issuing agency means an organization responsible for assigning a globally unique identifier to an enterprise, as indicated in the Register of Issuing Agency Codes for International Standards Organization/International Electrotechnical Commission 15459, located at http://www.aimglobal.org/?Reg_Authority15459.

Item type means a coded representation of the description of the item being warranted, consisting of the codes C--component procured separate from end item, S--subassembly procured separate from end item or subassembly, E--embedded in component, subassembly or end item parent, and P--parent end item.

Starting event means the event or action that initiates the warranty, such as first use or upon installation.

Serialized item means each item produced is assigned a serial number that is unique among all the collective tangible items produced by the enterprise, or each item of a particular part, lot, or batch number is assigned a unique serial number within that part, lot, or batch number assignment within the enterprise identifier. The enterprise is responsible for ensuring unique serialization within the enterprise identifier or within the part, lot, or batch numbers, and that serial numbers, once assigned, are never used again.

Unique item identifier means a set of data elements marked on an item that is globally unique and unambiguous.

Usage means the quantity and an associated unit of measure that specifies the amount of a characteristic subject to the contractor's obligation to provide for remedy or corrective action, such as a number of miles, hours, or cycles.

Warranty administrator means the organization specified by the guarantor for managing the warranty.

Warranty guarantor means the enterprise that provides the warranty under the terms and conditions of a contract.

Warranty repair source means the organization specified by a warranty guarantor for receiving and managing warranty items that are returned by a customer.

Warranty tracking means the ability to trace a warranted item from delivery through completion of the effectivity of the warranty.

(b) Reporting of data for warranty tracking and administration.

(1) The Contractor shall provide the information required by the attachment entitled “Warranty Tracking Information” on each contract line item number, subline item number, or exhibit line item number for warranted items no later than the time of award. Information required in the warranty attachment shall include such information as duration, fixed expiration, item type, starting event, usage, warranty administrator

enterprise identifier, and warranty guarantor enterprise identifier.

(2) The Contractor shall provide the following information no later than when the warranted items are presented for receipt and/or acceptance--

(i) The unique item identifier for each warranted item required by the attachment entitled “Warranty Tracking Information;”" and

(ii) The warranty repair source information and instructions for each warranted item required by the attachment entitled “Source of Repair Instructions.”

(3) The Contractor shall submit the data for warranty tracking to the Contracting Officer with a copy to the requiring activity and the Contracting Officer Representative.

(4) For additional information on warranty attachments, see the “Warranty and Source of Repair” training and “Warranty and Source of Repair Tracking User Guide” accessible on the Product Data Reporting and Evaluation Program (PDREP) Web site at https://www.pdrep.csd.disa.mil/pdrep_files/other/wsr.htm.

(c) Reservation of rights. The terms of this clause shall not be construed to limit the Government's rights or remedies under any other contract clause.

(End of clause)

252.247-7023 TRANSPORTATION OF SUPPLIES BY SEA (APR 2014)

(a) Definitions. As used in this clause --

"Components" means articles, materials, and supplies incorporated directly into end products at any level of manufacture, fabrication, or assembly by the Contractor or any subcontractor.

"Department of Defense" (DoD) means the Army, Navy, Air Force, Marine Corps, and defense agencies.

"Foreign-flag vessel" means any vessel that is not a U.S.-flag vessel.

"Ocean transportation" means any transportation aboard a ship, vessel, boat, barge, or ferry through international waters.

"Subcontractor" means a supplier, materialman, distributor, or vendor at any level below the prime contractor whose contractual obligation to perform results from, or is conditioned upon, award of the prime contract and who is performing any part of the work or other requirement of the prime contract.

"Supplies" means all property, except land and interests in land, that is clearly identifiable for eventual use by or owned by the DoD at the time of transportation by sea.

(i) An item is clearly identifiable for eventual use by the DoD if, for example, the contract documentation contains a reference to a DoD contract number or a military destination.

(ii) "Supplies" includes (but is not limited to) public works; buildings and facilities; ships; floating equipment and vessels of every character, type, and description, with parts, subassemblies, accessories, and equipment; machine tools; material; equipment; stores of all kinds; end items; construction materials; and components of the foregoing.

"U.S.-flag vessel" means a vessel of the United States or belonging to the United States, including any vessel

registered or having national status under the laws of the United States.

(b)(1) The Contractor shall use U.S.-flag vessels when transporting any supplies by sea under this contract.

(2) A subcontractor transporting supplies by sea under this contract shall use U.S.-flag vessels if--

(i) This contract is a construction contract; or

(ii) The supplies being transported are--

(A) Noncommercial items; or

(B) Commercial items that--

(1) The Contractor is reselling or distributing to the Government without adding value (generally, the Contractor does not add value to items that it contracts for f.o.b. destination shipment);

(2) Are shipped in direct support of U.S. military contingency operations, exercises, or forces deployed in humanitarian or peacekeeping operations; or

(3) Are commissary or exchange cargoes transported outside of the Defense Transportation System in accordance with 10 U.S.C. 2643.

(c) The Contractor and its subcontractors may request that the Contracting Officer authorize shipment in foreign-flag vessels, or designate available U.S.-flag vessels, if the Contractor or a subcontractor believes that --

(1) U.S.-flag vessels are not available for timely shipment;

(2) The freight charges are inordinately excessive or unreasonable; or

(3) Freight charges are higher than charges to private persons for transportation of like goods.

(d) The Contractor must submit any request for use of foreign-flag vessels in writing to the Contracting Officer at least 45 days prior to the sailing date necessary to meet its delivery schedules. The Contracting Officer will process requests submitted after such date(s) as expeditiously as possible, but the Contracting Officer's failure to grant approvals to meet the shipper's sailing date will not of itself constitute a compensable delay under this or any other clause of this contract. Requests shall contain at a minimum --

(1) Type, weight, and cube of cargo;

(2) Required shipping date;

(3) Special handling and discharge requirements;

(4) Loading and discharge points;

(5) Name of shipper and consignee;

(6) Prime contract number; and

(7) A documented description of efforts made to secure U.S.-flag vessels, including points of contact (with names and telephone numbers) with at least two U.S.-flag carriers contacted. Copies of telephone notes, telegraphic and facsimile message or letters will be sufficient for this purpose.

(e) The Contractor shall, within 30 days after each shipment covered by this clause, provide the Contracting Officer and the Maritime Administration, Office of Cargo Preference, U.S. Department of Transportation, 400 Seventh Street SW., Washington, DC 20590, one copy of the rated on board vessel operating carrier's ocean bill of lading, which shall contain the following information:

(1) Prime contract number;

(2) Name of vessel;

(3) Vessel flag of registry;

(4) Date of loading;

(5) Port of loading;

(6) Port of final discharge;

(7) Description of commodity;

(8) Gross weight in pounds and cubic feet if available;

(9) Total ocean freight in U.S. dollars; and

(10) Name of the steamship company.

(f) If this contract exceeds the simplified acquisition threshold, the Contractor shall provide with its final invoice under this contract a representation that to the best of its knowledge and belief--

(1) No ocean transportation was used in the performance of this contract;

(2) Ocean transportation was used and only U.S.-flag vessels were used for all ocean shipments under the contract;

(3) Ocean transportation was used, and the Contractor had the written consent of the Contracting Officer for all foreign-flag ocean transportation; or

(4) Ocean transportation was used and some or all of the shipments were made on foreign-flag vessels without the written consent of the Contracting Officer. The Contractor shall describe these shipments in the following format:

ITEM DESCRIPTION	CONTRACT LINE ITEMS	QUANTITY
TOTAL		

(g) If this contract exceeds the simplified acquisition threshold and the final invoice does not include the required representation, the Government will reject and return it to the Contractor as an improper invoice for the purposes of the Prompt Payment clause of this contract. In the event there has been unauthorized use of foreign-flag vessels in the performance of this contract, the Contracting Officer is entitled to equitably adjust the contract, based on the unauthorized use.

(h) In the award of subcontracts for the types of supplies described in paragraph (b)(2) of this clause, including subcontracts for commercial items, the Contractor shall flow down the requirements of this clause as follows:

(1) The Contractor shall insert the substance of this clause, including this paragraph (h), in subcontracts that exceed the simplified acquisition threshold in part 2 of the Federal Acquisition Regulation.

(2) The Contractor shall insert the substance of paragraphs (a) through (e) of this clause, and this paragraph (h), in subcontracts that are at or below the simplified acquisition threshold in part 2 of the Federal Acquisition Regulation.

(End of clause)

252.247-7024 Notification of Transportation of Supplies by Sea (MAR 2000)

(a) The Contractor has indicated by the response to the solicitation provision, Representation of Extent of Transportation by Sea, that it did not anticipate transporting by sea any supplies. If, however, after the award of this contract, the Contractor learns that supplies, as defined in the Transportation of Supplies by Sea clause of this contract, will be transported by sea, the Contractor --

(1) Shall notify the Contracting Officer of that fact; and

(2) Hereby agrees to comply with all the terms and conditions of the Transportation of Supplies by Sea clause of this contract.

(b) The Contractor shall include this clause; including this paragraph (b), revised as necessary to reflect the relationship of the contracting parties--

(1) In all subcontracts under this contract, if this contract is a construction contract; or

(2) If this contract is not a construction contract, in all subcontracts under this contract that are for--

(i) Noncommercial items; or

(ii) Commercial items that--

(A) The Contractor is reselling or distributing to the Government without adding value (generally, the Contractor does not add value to items that it subcontracts for f.o.b. destination shipment);

(B) Are shipped in direct support of U.S. military contingency operations, exercises, or forces deployed in humanitarian or peacekeeping operations; or

(C) Are commissary or exchange cargoes transported outside of the Defense Transportation System in accordance with 10 U.S.C. 2643.

(End of clause)

Section J - List of Documents, Exhibits and Other Attachments

EXHIBITS/ATTACHMENTS

DOCUMENT TYPE	DESCRIPTION
Exhibit A	Contract Data Requirements List (CDRL) – DD Form 1423
Attachment 1	Quality Assurance Surveillance Plan (QASP)
Attachment 2	Contract Security Classification Specification – DD Form 254
Attachment 3	Wage Determination, 2015-4427, Rev 9
Attachment 4	Software Licensing Disclosure
Attachment 5	CDRL A006/A007, Attach 1 – Staffing Plan
Attachment 6	CDRL A009, Attach 1 – CSWF Report

Distribution Table

Contractor: Praescient Analytics, LLC 635 Slaters Lane, Suite 200 Alexandria, VA 22314 POC: Katie Crotty, CEO katie@praescientanalytics.com 703-739-2110	**DFAS HQ0338** **DCMA S2404A** **All electronically distributed.**
SPAWARSYSCEN Atlantic Points of Contact: Contract Offier's Representative: (b)(6) (b)(6)@navy.mil Contract Administration Team POC: Terrie Johnson Terrie.johnson@navy.mil Ordering Team POC: Shauna Tangemann Shauna.tangemann@navy.mil	